Università
Ca'Foscari
Venezia

Corso di Laurea magistrale in
Economia e Finanza

Tesi di Laurea

La cyber insurance per gestire il cyber security risk

Relatrice
Ch.ma Prof.ssa Antonella Basso

Laureando
Filippo Petrelli
Matricola 871307

Anno Accademico
2018 / 2019

INDICE

INTRODUZIONE

La globalizzazione e l'innovazione tecnologica del nuovo millennio hanno aperto strade un tempo impensabili nel campo della telecomunicazione, nella fluidità dei processi, nella logistica, nelle attività emergenti e nelle nuove opportunità di sviluppo. Tutto ciò comporta da una parte alcuni traguardi innegabili e dall'altra nuovi rischi che vanno puntualmente individuati, monitorati rigorosamente e quindi gestiti in modo adeguato.
Le imprese diventano sempre più vulnerabili alle minacce informatiche a causa della crescente dipendenza da computer, reti, programmi, social media e dati a livello globale. Il cyber risk rappresenta la potenziale perdita o danno correlato all'infrastruttura tecnica, all'uso della tecnologia o alla reputazione di un'organizzazione; questo particolare rischio può a sua volta essere suddiviso in due ulteriori categorie di rischio:

- il rischio IT puro che comprende i rischi derivanti da eventi accidentali sui sistemi IT, quali l'incendio, il guasto elettrico, l'errore umano o una problematica software;
- cyber attack inteso come rischio collegato alle attività criminali commesse con dolo da un soggetto terzo mediante l'uso della rete. Tali attacchi informatici sono generalmente volti ad accedere, modificare o distruggere informazioni sensibili, estorcere denaro o interrompere i normali processi aziendali.

Focalizzandoci su quest'ultima categoria di rischio, è doveroso riferirsi alla cyber security, ossia la pratica di proteggere sistemi, reti e programmi dai cyber attack. L'implementazione di efficaci misure di sicurezza informatica è oggi particolarmente impegnativa poichè ci sono più dispositivi rispetto al numero di persone e gli aggressori diventano via via più innovativi e aggressivi.
In ogni caso, la presenza di sistemi di sicurezza non sostituisce l'assicurazione informatica nota come cyber insurance. I sistemi possono fallire, l'errore umano si può verificare e gli hacker escogitano spesso un modo per violare non solo la tecnologia aziendale ma anche le soluzioni di sicurezza adottate.
È possibile, tuttavia, beneficiare sia della cyber security, che della cyber insurance, infatti le misure di sicurezza informatica sono quasi sempre un prerequisito per la copertura cyber assicurativa e la presenza di una valida strategia di sicurezza informatica potrebbe ridurre i costi dei premi assicurativi.

Questo percorso presenta un quadro relativo alle possibili modalità di modellizzazione e pricing del cyber risk, soffermandosi in maniera particolare sul modello Copula, teorizzato da Herath S. ed Herath T., attraverso il quale si giunge, utilizzando il software statistico R, ad un prospetto di tariffazione del premio per la cyber insurance; successivamente si effettua un confronto tra i risultati ottenuti mediante i dati del 2005 e gli esiti derivanti dai dati del 2018.

Nel primo capitolo è stata introdotta la nozione di cyber crime, volendo evidenziare particolarmente la crescita di questa tipologia di crimini essendo facilmente attuabili, con scarse probabilità di cattura e che portano con sé un notevole profitto. Il cyber crime ha notevoli impatti in termini di costi, ma a causa di problemi di stima e costi nascosti, risulta difficile poterli quantificare in modo preciso. La seconda parte del capitolo si concentra sul cyber attack descrivendo i cinque più pericolosi attacchi informatici del 2019.

Il secondo capitolo segue il naturale sviluppo di quello precedente e si focalizza su come le imprese si attivino per affrontare il cyber crime dopo averlo individuato come problema emergente. Questa parte di lavoro cerca di mettere in allarme coloro che, nel 2019 possiedono ancora un sistema di sicurezza informatica obsoleto o addirittura ne sono sprovvisti; tutto ciò grazie ai dati forniti dai numerosi report relativi alla situazione attuale delle imprese nell'ambito della cyber security. Gli studi mostrano che il 53 % delle aziende non è al passo con i tempi. Successivamente è stato descritto il GDPR (General Data Protection Regulation), cioè il regolamento scritto dall'Unione Europea ed entrato in vigore nel 2018 al fine di modernizzare le leggi che proteggono le informazioni personali; a tal proposito le imprese dovrebbero seguire dodici passi per conformarsi a tale regolamento con l'intento di evitare le sanzioni ad esso associate.

Il terzo capitolo apre le porte al concetto di cyber insurance mettendo in luce le caratteristiche dei vari tipi di copertura (copertura di prima parte, copertura di terze parti, copertura retroattiva), comprese le innumerevoli garanzie accessorie. Per l'impresa risulta complicato ricercare la giusta copertura assicurativa, quindi è rilevante conoscere, evitando i vari passi falsi che potrebbero compromettere tale copertura. L'ultimo punto analizzato nel capitolo riguarda la relazione tra la cyber insurance e il GDPR.

Nel quarto capitolo vengono trattati la modellizzazione e il pricing del cyber security risk sul piano teorico. Poiché queste problematiche non sono ancora concluse, è stato dato credito a tutti gli studiosi che hanno analizzato questo argomento dando particolare attenzione a tre lavori significativi:

- il lavoro di Maochao e Lei che utilizzano processi stocastici (Markov e non-Markov) per descrivere le dinamiche della diffusione dell'epidemia nel tempo;
- lo studio di Verlaine M. che propone di estrarre informazioni afferenti al cyber risk da prodotti finanziari strutturati;
- il modello di pricing della cyber insurance basato sulle funzioni Copula di Herath H. ed Herath T.

Infine, nel quinto capitolo sono state riportate alcune applicazioni empiriche. Nella prima parte sono stati esaminati i modelli SIS e SIR, ovvero due tipologie di modelli epidemici accostati al modello Markov di Machao e Lei. Quindi, si prosegue introducendo il concetto di funzione Copula e ne viene presentato il funzionamento attraverso una semplice simulazione con il software R. Infine, grazie ai dati riguardanti il tipo di virus e le relative perdite trovati all'interno dello studio delle sorelle Herath, viene simulato il pricing del premio della cyber insurance. Poiché i dati sono stati rilevati nel 2005, si effettua un'ulteriore simulazione relativa all'anno 2018 raccogliendo le informazioni dal "Cyber claims report (O'Connor, 2019).

Come ultima fase vengono comparati i risultati ottenuti per i due diversi istanti temporali, giungendo ad importanti conclusioni illustrate alla fine del lavoro.

Capitolo 1

1. UN PROBLEMA EMERGENTE: IL CYBER CRIME

1.1. IL CYBER CRIME: IMPATTO E RAGIONI DI CRESCITA

Il nostro mondo ormai non può più prescindere da internet, miliardi di individui si connettono alla rete attraverso diversi dispositivi, lo considerano un bisogno primario. Viviamo in una realtà di orologi connessi agli smartphone che consentono tra le tante cose il monitoraggio del battito cardiaco, di applicazioni che svolgono lavoro contabile mediante l'invio di semplici foto di ricevute, di macchine che si auto-guidano (Uber), criptovalute...

I big data sono il cuore pulsante di questi straordinari sviluppi, tanto è vero che ogni tipo di dispositivo elettronico può raccogliere una vasta gamma di informazioni e tale sistema opera sia a favore che contro: da un lato cerca di esplorare al meglio la persona per analizzarne i bisogni e quindi cercare di soddisfarli, dall'altro tenta di manipolarla al fine di sedurla con nuovi desideri[1] (Ryu, 2014). Questa interazione e raccolta avviene ogni giorno: le compagnie pagano piccole somme per acquisire i dati mentre alcuni privi di scrupoli cercano di procurarseli (Walker, 2019).

Gli hacker rappresentano lo spettro di questo delicato argomento, venendo spesso definiti criminali anche se esistono hacker “etici” che aiutano le aziende a determinare il livello di vulnerabilità del sistema offrendo consigli per rafforzare la sicurezza (Gupta, 2019). La parola in sé suscita sempre e unicamente sentimenti negativi tra la gente, comunque il vero significato è quello di investigazione. L’hacker infatti apprende tutti i dettagli riguardanti un determinato sistema individuando le possibilità di eluderne le difese e impiegando tempo e risorse per sfruttare qualsiasi tipo di vulnerabilità: viene a conoscenza di tutto ciò che la maggior parte delle persone ignora (Vegh, 2002). Non esistono informazioni sicure, il cybercrime impatta principalmente sulle attività di business e tecnologie emergenti che, in questa fase di trasformazione globale, sono imprescindibili. Gli hacker ci hanno dimostrato che è possibile compromettere auto a guida autonoma, accedere a sistemi avionici durante il volo e che dispositivi come i

[1] Per esempio, indirizza a comprare un determinato prodotto online o scaricare una certa app.

microinfusori e pacemaker sono vulnerabili; quindi, come possiamo pretendere sicurezza da applicazioni e processi avanzati quando non sono affidabili neanche quelli fondamentali per il business (Guo, 2016)?

Nel corso dell'ultimo periodo il crimine informatico, essendo una forma di reato facilmente attuabile, gratificante e con scarse probabilità di cattura, è aumentato notevolmente, giungendo a divenire la terza attività criminale per impatto sul prodotto interno lordo mondiale (0,8%) dietro solo alla corruzione governativa (1,2 %) e al traffico di droga (0,89%) (Hale, 2018). Un recente rapporto del CSIS (Center for strategic & international studies) mostra che questo impatto è in aumento da 445 miliardi nel 2014 a 600 miliardi nel 2018; dietro a tale crescita c'è l'adozione da parte dei criminali informatici di nuove tecnologie e lo sfruttamento di mercati neri e criptovalute. In tale rapporto è stata riscontrata la difficoltà nel cercare di monetizzare il crimine informatico, in particolare il furto di IP (intellectual property) può distorcere le stime: i criminali non sempre guadagnavano l'intero valore di ciò che avevano rubato.

Secondo una buona stima i due terzi delle persone online (più di due miliardi di individui) sono stati oggetto di furto e compromissione delle informazioni online e un sondaggio rivelò che il 64% degli americani era stato vittima di addebiti fraudolenti o perdita di informazioni personali.

Basso rischio e profitti elevati sono i punti di forza di questo particolare reato, tanto è vero che un cyber criminale può guadagnare centinaia di migliaia o addirittura milioni di dollari; inoltre ripensando a grandi crimini informatici, da Target a SWIFT a Equifax, nessuno degli autori è stato perseguito fino ad oggi, poiché le forze dell'ordine possono essere efficienti e abili nel cercare di raggiungere i criminali informatici, ma diversi operano fuori dalla loro portata (Antonucci, 2017).

Le ragioni della crescita di questo tipo di crimine sono le seguenti (Lewis, 2018):

- adozione rapida di nuove tecnologie da parte dei criminali informatici;
- aumento del numero di nuovi utenti online (provenienti da paesi a basso reddito con debole sicurezza informatica);
- maggior facilità nel commettere crimini informatici, con la crescita del cyber crime come servizio;
- numero sempre più crescente di "centri" di criminalità informatica che ora includono Brasile, India, Corea del Nord e Vietnam;

- crescente sofisticazione finanziaria tra gli alti livelli di criminalità informatica che, rende la monetizzazione più semplice.

La monetizzazione dei dati rubati è sempre stato un problema per i criminali informatici e ciò ora risulta più semplice a causa dei miglioramenti nel mercato nero e grazie all'uso delle valute digitali. All'interno del dark web vengono offerti in gran quantità numeri di carte di credito e informazioni di identificazione personale (PII) utilizzando una serie complessa di transazioni che coinvolgono broker e altri intermediari, in tal modo il furto finanziario viene in seguito trasferito sui conti bancari dei criminali attraverso transazioni destinate a mascherare e confondere. Tale facilità sussiste in relazione alle scarse misure di protezione adottate dalla maggior parte degli utenti, anche quelle più elementari, inoltre numerosi prodotti tecnologici non sono dotati di difese adeguate. Al contrario, i criminali informatici utilizzano una tecnologia avanzata finalizzata a identificare gli obiettivi, creano e consegnano automaticamente software e monetizzano ciò che è stato rubato.

Il report sulle minacce alla sicurezza di Internet di Symantec del 2019 ha rilevato che il 10% degli Url è dannoso, gli attacchi web sono aumentati del 56%, quelli alla supply chain del 78% e il 48 % degli allegati dannosi provengono da e-mail di lavoro. Il rapporto ha anche identificato che il numero di attacchi informatici di gruppo ha avuto un incremento del 25% con una media di 55 imprese colpite da ciascun attacco. Per la prima volta dal 2013, si nota una diminuzione dell'attività del ransomware[2], avvenuta durante il 2018, con il numero complessivo di infezioni in calo del 20%. Tuttavia, all'interno di queste cifre generali c'è stato un cambiamento drammatico: fino al 2017, i consumatori sono stati i più colpiti da ransomware, rappresentando la maggior parte delle infezioni, poi il saldo si è spostato verso le imprese[3]. Nel 2018, questo spostamento ha subito un'accelerazione (12%) e le aziende hanno rappresentato l'81% di tale contagio informatico. Una motivazione della tragica espansione può essere causata dal principale mezzo di comunicazione per le imprese, la posta elettronica, che rappresenta il principale strumento di propagazione degli attacchi informatici; inoltre, un numero crescente di consumatori utilizza esclusivamente dispositivi mobili e i loro dati essenziali sono spesso sottoposti a backup nel cloud.

Un altro fattore che contribuisce al declino è dato dalla perdita di interesse nel ransomware da parte di molti gruppi di cybercriminali, che sono passati alla consegna di

[2] Per maggiore chiarezza sui vari tipi di attacchi informatici si veda il paragrafo 1.3 intitolato "Che cos'è un cyber attack?".

[3] Ulteriori informazioni e dati sono presenti nel report "Threat attack!" di Symantec del Febbraio 2019.

altri tipi di malware come Trojan bancari e furti di informazioni.

Il cybercrime agisce su vasta scala e la quantità di attività fraudolente su Internet è sbalorditiva: uno dei più grandi fornitori di servizi Internet (ISP) segnala 80 miliardi di scansioni dannose al giorno, risultato di sforzi automatizzati dei criminali informatici al fine di identificare obiettivi vulnerabili.

Il phishing rimane il modo più popolare e più semplice di commettere un crimine informatico, con il gruppo di lavoro anti-phishing (APWG) che ha registrato nel 2016 oltre 1.2 milioni di attacchi, molti di essi collegati a ransomware (Lewis, 2018). La Privacy Rights Clearing House invece stima 4,8 i miliardi di record persi come risultato di violazioni dei dati nel 2016.

Figura 1.1: Stima dell'attività giornaliera da parte della criminalità informatica.

Cybercrime	Stima dell'attività giornaliera
Scansioni maligne	80 miliardi
Nuovi malware	300,000
Phishing	33,000
Ransomware	4,000
Dati persi a causa di hackeraggio	780,000

Fonte: The Economic Impact of Cybercrime (Grobman, 2018).

La ricerca di ISACA[4] riconosce che le imprese sono più consapevoli del rischio di minacce persistenti e avanzate (APT[5]) e stanno prendendo provvedimenti per gestire al meglio questo rischio, ma si affidano prevalentemente ai tradizionali meccanismi di difesa e rilevamento che possono essere inefficaci contro le minacce costanti.

Inoltre, mentre sono possibili intrusioni Web derivanti dalla configurazione o da altri cali di sicurezza, vi è una propensione sempre più intensa ad attaccare i dispositivi mobili con un incremento del 33% delle vulnerabilità mobili rispetto al 2017 e si prevede un'ulteriore crescita del crimine informatico per quanto riguarda l'hackeraggio dell'IoT (internet of things), dispositivi che, pur non essendo particolarmente preziosi, forniscono nuovi e facili approcci per rubare informazioni personali o ottenere l'accesso a dati o reti di valore

[4] Information Systems Audit and Control Association.
[5] Advanced Persistent Threat.

(Iagolnitzer et al., 2013).

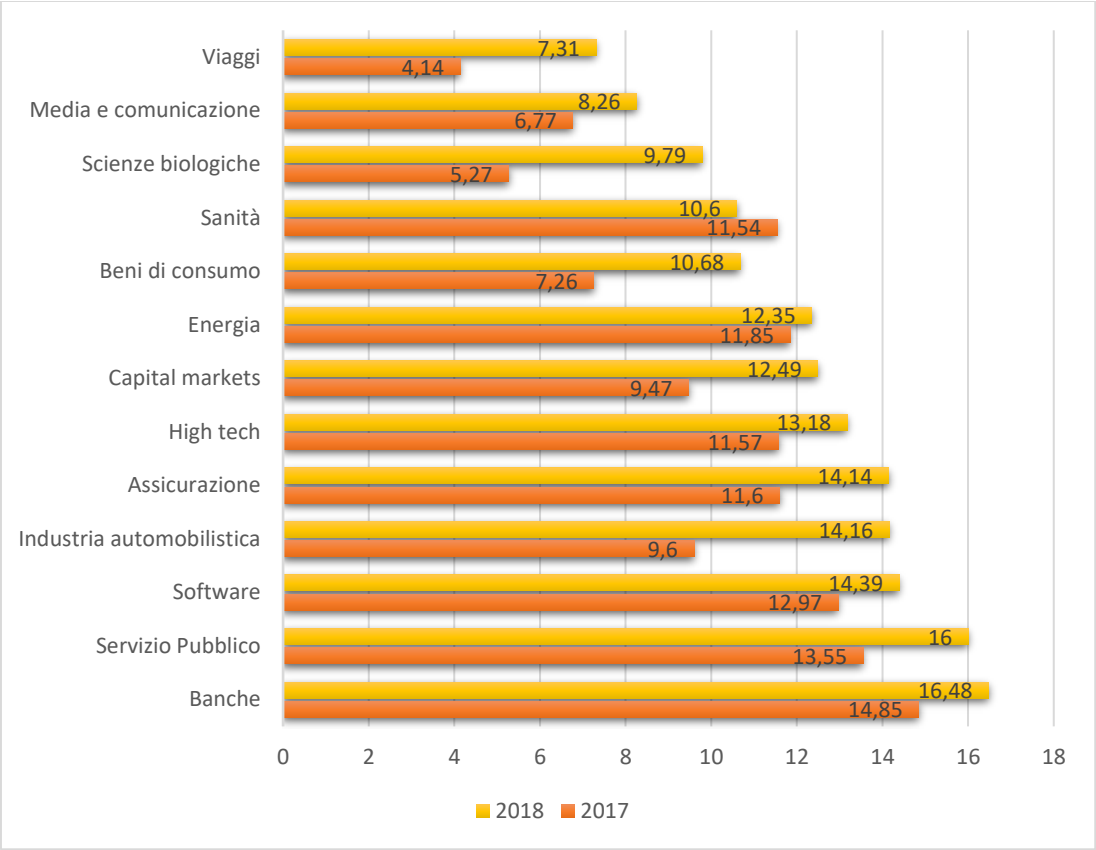
“Ammettere di avere un problema rappresenta il primo passo verso la sua risoluzione”, anche in questo caso la consapevolezza del problema informatico e dell’impatto sulle imprese rappresenta solo un piccolo passo, ma siamo molto distanti dal risolverlo. È necessario un ripensamento di come le informazioni e la sicurezza informatica siano governate, gestite e implementate, quindi si tratta di scegliere un approccio più olistico e incentrato sul business alla cybersecurity che deve perciò essere riconosciuta come un problema commerciale e non solo tecnico.

1.2. IL COSTO GLOBALE DEL CRIMINE INFORMATICO

L’aumento degli attacchi e del tempo di contenimento del danno a seguito di violazioni hanno provocato inevitabilmente una continua crescita del costo del crimine informatico. Le imprese stanno assistendo a un costante aumento del numero di violazioni[6] della sicurezza, da 130 nel 2017 a 145 nel 2018 tradotto in incremento del costo totale per ciascuna società da 10.5 milioni di euro nel 2017 a 11.7 milioni nel 2018 (12% di crescita). La dettagliata analisi svolta dall’istituto Ponemon in collaborazione con Accenture Security mostra che le industrie bancarie e dei servizi pubblici continuano ad avere il più alto costo del crimine informatico con un aumento rispettivamente dell'11% e del 18%.
Il settore energetico è rimasto piuttosto piatto nel corso dell'anno con un piccolo aumento del 4%, mentre la sanità ha registrato un leggero calo nei costi della criminalità di circa 9 punti percentuali.

[6] Una violazione della sicurezza è quella che provoca l'infiltrazione delle reti principali o dei sistemi aziendali di un'azienda, escludendo quindi la pletora di attacchi fermati dalle difese del firewall di un'azienda.

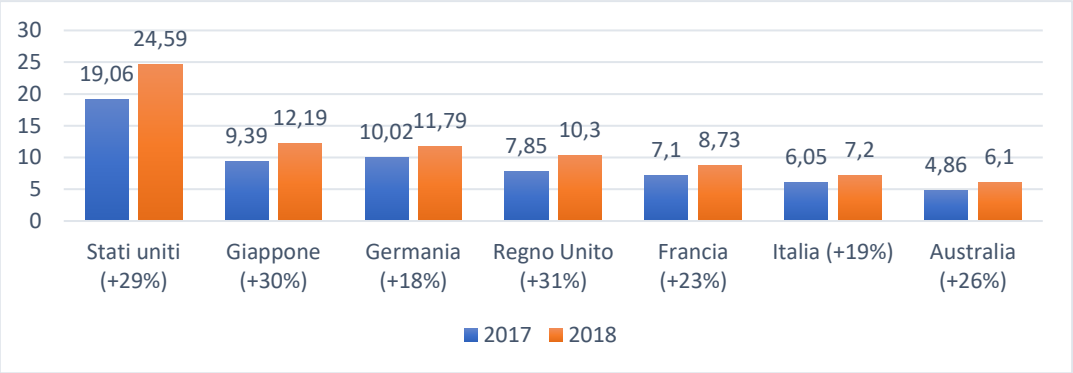
Figura 1.2: Costo medio del cybercrime per settore in mln di euro.



Fonte: Report "The cost of cybercrime" di Accenture security (Bissell, 2019).

Questo studio svolto a livello mondiale vede gli Stati Uniti in cima alla lista con un costo medio annuo del crimine informatico in aumento del 29% nel 2018, ma l'incremento più elevato (31%) è stato registrato da imprese del Regno Unito che sono cresciute fino a 10.3 milioni di euro, seguite dal Giappone che ha subito un aumento del 30%. L'Italia ha visto un incremento del 19% mentre la Germania, grazie ai numerosi investimenti svolti dalle aziende tedesche nel 2017, si piazza all'ultimo posto con una crescita di "soli" 18 punti percentuali.

Figura 1.3: Costo medio del cybercrime per paese.



Fonte: Report "The cost of cybercrime" di Accenture security (Bissell, 2019).

Gli elementi del crimine informatico che hanno impatti in termini di costi includono (Lewis, 2018):

- la perdita di proprietà intellettuale e informazioni confidenziali di business;
- frodi online e reati finanziari, spesso risultato di furto di informazioni di identificazione personale (PII);
- manipolazione finanziaria utilizzando il furto di informazioni sensibili riguardanti potenziali fusioni o conoscenze anticipate di relazioni sulle prestazioni per le società quotate in borsa;
- costi opportunità, inclusa l'interruzione della produzione o servizi e un deterioramento della fiducia per le attività online (questo include l'effetto del ransomware che coinvolge i pagamenti per riscattare dati crittografati e soprattutto gravi interruzioni dei servizi e della produzione);
- il costo per proteggere le reti, acquistando cyber insurance e/o pagando per il recupero dagli attacchi informatici;
- danni alla reputazione e rischio di responsabilità per la società hackerata e il suo marchio, inclusi i danni temporanei al valore delle scorte. Le stime del costo del crimine informatico continuano a essere significative.

Il costo del crimine informatico è distribuito in modo non uniforme tra tutti i paesi del mondo, difatti sono state trovate variazioni in relazione alla regione, ai livelli di reddito e al livello di maturità della sicurezza informatica. Non sorprende che più ricco è il paese, maggiore è la probabilità che si verifichi una perdita a causa della criminalità informatica. Le maggiori perdite (in percentuale del reddito nazionale) si verificano nelle nazioni di

livello intermedio, cioè quelle che sono digitalizzate, ma non ancora pienamente capaci dal punto di vista della sicurezza informatica.

Figura 1.4: Distribuzione del cybercrime nel 2017.

Regione	Costo del cybercrime in mld di euro	Perdita in % del PIL
America del nord	da 126 a 158	da 0.69 a 0.87
Europa e Asia centrale	da 144 a 162	da 0.79 a 0.89
Asia dell'est e Pacifico	da 108 a 180	da 0.53 a 0.89
Asia del sud	da 6 a 14	da 0.24 a 0.52
America latina e Caraibi	da 14 a 27	da 0.28 a 0.57
Africa subsahariana	da 1 a 3	da 0.07 a 0.2
Medio Oriente e Nord Africa	da 2 a 5	da 0.06 a 0.16
Totale	da 401 a 549	da 0.59 a 0.8

Fonte: The Economic Impact of Cybercrime (Grobman, 2018).

La società americana di cybersecurity "riskIQ" ha rilasciato nel 2019 il report "Evil internet minute" in cui analizza gli eventi avvenuti in rete nel 2018 per ogni singolo minuto:

- 2.6 milioni di euro di ricavi ottenuti dal crimine informatico;
- 22.50 euro di danni causati da violazioni nei confronti delle maggiori imprese;
- 1,730 euro originati da hackeraggio su scambi di criptovalute;
- 15,876 euro persi a causa di phishing:
- 8,100 dati persi o compromessi;
- 4 imprese cadute vittima di ransomware;
- 0.32 app entrate nella blacklist;
- 2.4 siti phishing creati.

La lettura di questi dati è un caldo invito per le imprese a porre la sicurezza informatica come competenza chiave e integrata in tutto ciò che un'azienda fa e rappresenta poiché, dalle persone, ai dati, alle tecnologie, ogni aspetto di un'azienda invita al rischio. Nonostante i loro investimenti, i leader aziendali devono ancora migliorare il valore

economico dalle loro strategie di sicurezza informatica.

1.2.1. PROBLEMI DI STIMA

Qualsiasi stima del costo del crimine informatico deve affrontare diverse problematiche; in primo luogo, la sottostima da parte delle vittime e la scarsità di raccolta dei dati da parte dei governi, che possono facilmente rivelare il numero di furti d'auto o persino di francobolli, ma non il numero riguardante il crimine online (Lewis, 2018).
Un ulteriore errore è aggravato dalla riluttanza da parte di molte aziende a riferire se e quando sono state vittime.
La documentazione rimane così un problema e le stime nazionali sono ancora notevolmente imprecise, poichè viene riportata solo una frazione delle perdite dal momento che le società cercano di evitare rischi di responsabilità e danni alla reputazione.
In secondo luogo, è difficile stimare il costo di aggirare il rischio della rete, dove le persone scelgono di tornare alla carta e rifuggono le transazioni online, poiché temono il crimine informatico. In generale, l'attrattiva delle tecnologie digitali è ancora troppo convincente per portare persone e aziende a rinunciare a Internet, ma ci sono segni di cambiamento incipiente.
In terzo luogo, un grosso problema con il costo stimato è che esso fornisce anche quello aggregato ai paesi, trascurando le aziende individuali o i consumatori e non denuncia una distribuzione distorta quando si tratta di vittime.
Il crimine è una "normale" parte dell'interazione sociale e degli affari internazionali e i governi adottano le misure individualmente e in modo cooperativo per gestire e ridurre il suo costo. Il presupposto è che il crimine informatico rispecchi altre attività criminali:

- pirateria marittima: una stima indica che il costo annuale della pirateria si aggirava tra 5,1 e 5,5 miliardi di euro nel 2012 giungendo nel 2016 a 3,8 miliardi per la sola Africa;
- pilferage: le aziende accettano il "furto" come parte del costo per fare affari; utilizzando i tassi di furto come analogia, il costo del crimine informatico negli Stati Uniti è tra lo 0,5% e 2% del reddito nazionale;
- criminalità transnazionale: l'Ufficio delle Nazioni Unite contro la droga e il crimine ha stimato il costo di tutte le organizzazioni transnazionali di criminalità pari a 785 miliardi di euro nel 2012, 1,2% del PIL globale di cui seicento miliardi

provenienti dal traffico di droga;

- il World Economic Forum[7] ha valutato il costo totale del crimine globale di 1,6 triliardi, circa l'1,5% del PIL globale.

Nel 2016 è stato venduto 1 miliardo di dollari in assicurazione sulla sicurezza informatica[8], solo una piccola frazione rispetto alle centinaia di miliardi spesi per incendio o assicurazione marittima.

Il costo per la singola vittima può essere basso, con poche eccezioni, tanto è vero che molti consumatori, sebbene preoccupati, scrollano le spalle davanti al rischio e parecchie grandi aziende vedono la perdita finanziaria da hacking come un prezzo da pagare per fare affari online. L'Istituto Ponemon stima che il costo medio di una violazione sia di 3,3 milioni di euro quindi doloroso, ma non paralizzante per le grandi aziende poiché il vero rischio risiede nel danno al marchio e nell'aumento del rischio di responsabilità, così le grandi aziende hanno l'abitudine di 'autoassicurarsi', azzardando il fatto che qualsiasi perdita sarà gestibile.

Forse questo tipo di tolleranza, combinato con la sottostima, è uno dei motivi per cui il crimine informatico rimane così pervasivo.

1.2.2. FURTO DI PROPRIETA' INTELLETTUALE

L'area più importante per l'impatto del crimine informatico è il furto di informazioni confidenziali e proprietà intellettuale, che rappresenta qualsiasi innovazione creativa o commerciale che abbia valore economico o un qualsiasi segno distintivo[9] (Antonucci, 2018).

Il furto di IP (Intellectual Property) va ben oltre le tradizionali aree di interesse per i governi, come le tecnologie militari; un modo per misurare il suo impatto è quello di cercare prodotti concorrenti che prendono quote di mercato dai legittimi proprietari. Questo particolare reato impatta per almeno un quarto sul costo del crimine informatico e, quando coinvolge la tecnologia militare crea rischi anche per la sicurezza nazionale con perdite che possono spesso essere invisibili alla vittima, che, avendo ancora accesso

[7] Utilizzando i dati del 2011.

[8] Secondo un calcolo della National Association of Insurance Commissioners.

[9] Un esempio può essere un nome, un simbolo, un logo utilizzato nelle pratiche commerciali, idee e proprietà protette da leggi, marchi, brevetti o copyright, segreti commerciali, elenchi di clienti, invenzioni meccaniche, poesie, foto, musica, poesie…

all'IP copiata dai criminali, può attribuire un calo delle entrate alla concorrenza crescente anziché al furto (Lewis, 2018).

La Cina è al centro delle preoccupazioni relative ai furti di proprietà intellettuale, infatti prima del 2015 essa era responsabile di metà del cyber spionaggio contro gli Stati Uniti per quanto riguarda il furto di proprietà intellettuale e informazioni di valore commerciale causando una perdita annuale di 20 miliardi di dollari.

L'accordo di Obama-Xi[10] sul cyber spionaggio a fini commerciali, per mezzo del quale i due paesi concordarono tacitamente di poter continuare a spiarsi l'un l'altro previo accordo di una giustificazione di sicurezza nazionale. Tutto ciò avrebbe contribuito a far risparmiare agli Stati Uniti circa 15 miliardi di dollari in un anno; anche se, in base ad interviste con funzionari di vari paesi, il furto di IP continuerebbe senza sosta nonostante qualsiasi accordo.

Dare un valore all'IP è un'arte: le aziende possono stimare il loro flusso di entrate future che sarà capace di produrre il loro IP, ma un ladro potrebbe non essere in grado di farne un uso commerciale.

La migliore stima pone come valore di tutti gli IP negli Stati Uniti 12 trilioni di dollari (12 miliardi di miliardi), con un aumento annuo compreso tra 700 e 800 miliardi annuali. Sulla base delle precedenti analisi e supponendo che i tassi di perdita dovuti al furto di IP seguano altri tipi di crimine informatico e considerando l'effetto dell'accordo Obama-Xi, si stima che le perdite annuali per gli Stati Uniti ammontino a 10 e 12 miliardi (da 50 a 60 miliardi a livello globale) (Driggers, 2018).

Il furto di informazioni commerciali riservate per ottenere vantaggio nelle trattative o negli investimenti riveste una parte importante delle perdite dovute al crimine informatico, ma questo potrebbe non riflettere la perdita globale complessiva: il costo nascosto può provenire dall'uso di hacking per manipolare i prezzi delle azioni, tutto ciò, comunque, rimane difficile da rilevare.

[10] Al vertice di Xi-Obama del 2015, entrambi i leader hanno concordato che "il governo di nessuno dei due Paesi condurrà o supporterà consapevolmente il furto di proprietà intellettuale, inclusi segreti commerciali o altri dati riservati riguardanti informazioni commerciali con l'intento di fornire vantaggi competitivi per aziende o settori ".

1.2.3. COSTI NASCOSTI

La frode e il furto di proprietà intellettuale (IP) producono una grossa fetta della perdita dovuta al crimine informatico, ma è necessario considerare anche i costi di recupero, costi opportunità e la necessità di spendere di più per la sicurezza informatica. L'interruzione dell'attività commerciale è un costo correlato, spesso risultato di attacchi DDoS[11] e ransomware; in questi casi la perdita deriva dall'impedire a un'azienda di fare soldi, piuttosto che l'effettiva perdita di soldi.

Il 45% delle famiglie americane ha riferito che le preoccupazioni verso il crimine informatico hanno impedito loro di condurre transazioni finanziarie[12], acquisto di beni o servizi o registrazione su social network; nonostante il costo e il rischio effettivi possono essere bassi, la percezione del rischio sta rimodellando il comportamento delle persone su Internet, questo fatto danneggia la crescita economica. Detto questo, le persone in tutto il mondo sono così incantate dalle tecnologie digitali, che accettano il rischio come basso e ragionevole; i dirigenti consideravano il crimine informatico come "il costo di fare affari" mettendo al centro del loro interesse il danno reputazionale[13] piuttosto che le perdite effettive; sta cambiando come le pratiche aziendali e contabili assumono il rischio cibernetico.

Per comprendere l'effetto del crimine informatico bisogna confrontarlo con l'economia di Internet, stimata recentemente a 3,77 trilioni nel 2016. Usando questa cifra, possiamo associare il crimine informatico ad una tassa del 14% sulla crescita: ci sarebbero dei veri benefici allo sviluppo e alla prosperità in tutti paesi se la comunità internazionale decidesse di compiere uno sforzo per ridurlo (Driggers, 2018)

1.3. FINANCIAL CYBERCRIME

Per oltre un decennio le banche sono rimaste l'obiettivo preferito degli esperti criminali informatici, pertanto questo crimine comporta un costo elevato sulle istituzioni

[11] Distribuited Denial of Service, traducibile in italiano come "interruzione distribuita del servizio", consiste nel tempestare di richieste un sito fino a metterlo ko e renderlo così irraggiungibile (www.cybersecurity360.it)

[12] Secondo il sondaggio del Census Bureau (Smith, 2015) effettuato su un campione di 41000 famiglie nel 2014.

[13] In base ai risultati del sondaggio condotto da ISACA (Downs et al., 2019).

finanziarie che lottano per combattere la frode e le rapine. La ricerca[14] suggerisce che le imprese di servizi finanziari hanno rilevato la tensione proveniente dalla minaccia di attacchi informatici: le banche spendono in cybersecurity il triplo rispetto alle istituzioni non finanziarie poiché il crimine informatico pone a rischio "sistematico" la stabilità finanziaria. La protezione è elevata (sebbene siano necessarie riflessione e manutenzione continue) e sono in corso dei lavori per l'ottimizzazione della sicurezza. È necessario per questo settore il mantenimento in sicurezza dei dati, comunque esso necessita l'adeguamento a iniziative come: l'open banking che impone alle imprese la condivisione esterna e il mobile banking, tuttavia in circolazione troviamo molte false app che ingannano un consumatore su tre; inoltre continuano le truffe più tradizionali e, a peggiorare le cose c'è la maggior collaborazione tra hacker.

Nell'estate del 2018, l'FBI ha scoperto un attacco di massa a livello multinazionale nel settore bancario che ha svuotato in poche ore gli sportelli automatici.

Secondo il sondaggio svolto da ISACA[15](Downs, 2019):

- il 6% delle società di servizi finanziari afferma che la funzione di sicurezza delle informazioni attualmente soddisfa le esigenze della propria organizzazione, ma il 65% ha in programma di apportare dei miglioramenti fondamentali. Il problema emerso da tale sondaggio è che il 31% avverte un potenziale ostacolo nella carenza di abilità;
- le organizzazioni di questo settore sono maggiormente preoccupate per l'immaturità dei loro processi di sicurezza delle informazioni nelle aree di struttura finanziaria (citate come inesistenti o molto immature dal 18%), metriche e reportistica (18%) e gestione patrimoniale (17%);
- quasi 6 imprese su 10 (59%) hanno un centro operativo di sicurezza. È più probabile che eseguano le proprie funzioni internamente, che esternalizzandole: solo i test di penetrazione (79%) e la scienza digitale forense (52%) vengono maggiormente esternalizzati;
- solo il 16% delle società di servizi finanziari afferma che le loro comunicazioni sulla sicurezza delle informazioni soddisfano le loro esigenze (dato che pone il settore finanziario in testa per quanto riguarda le segnalazioni).

[14] Condotta da Symantec a proposito della sicurezza su internet nel 2019.

[15] EY global information security survey del 2019.

Tre paesi: Russia, Corea del Nord, e l'Iran sono i più attivi nell'hacking di istituzioni finanziarie, mentre la Cina rimane la più attiva nello spionaggio (Lewis, 2018).
Gli obiettivi dell'Iran sono effetti coercitivi, come evidenziato dall'attacco iraniano denial-of-service (DdoS) sulle principali banche statunitensi.
Il Nord Korean Reconnaissance General Bureau (RGB), come affermato dai ricercatori della sicurezza[16], ha sferrato svariati attacchi alle banche nei paesi in via di sviluppo rubando decine di milioni di dollari tramite l'invio di falsi ordini di pagamento. La Corea del Nord si è rivolta inoltre al furto di criptovalute per contribuire a finanziare il suo regime: i loro hacker hanno preso di mira almeno tre scambi di criptovaluta sudcoreani nel 2017 e l'Università della Scienza e tecnologia di Pyongyang ha iniziato ad offrire alla classe di studenti di informatica lezioni su Bitcoin e Blockchain, confermando il crescente interesse per le valute digitali.
Le maggiori istituzioni finanziarie internazionali investono in difesa, quale migliore prevenzione delle frodi e transazioni autenticate poiché le nazioni più sofisticate e i gruppi criminali organizzati hanno iniziato a prendere di mira le "cuciture" tra reti ben difese, sfruttando punti deboli nella rete finanziaria globale per portare a termine rapine enormi; la campagna nordcoreana per rubare il denaro attraverso la rete SWIFT è un ottimo esempio.
Riconoscendo la difficoltà nel realizzare furti di vasta portata su una singola grande banca occidentale, la RGB spostò l'obiettivo verso banche piccole, in via di sviluppo e meno sofisticate di paesi come il Bangladesh, il Vietnam e l'Ecuador. Dopo aver compromesso i sistemi di queste banche, hanno poi usato le credenziali delle vittime per inviare ciò che sembrava una legittima richiesta di trasferimento di fondi SWIFT a banche più grandi in altri paesi. Queste richieste sono apparse inizialmente legittime ai riceventi, dal momento che sono state inviate da banche partner quindi in alcuni casi il denaro è stato trasferito.
Il CSIS (Driggers, 2019) ritiene che la Russia sia in testa alla criminalità informatica, riflettendo l'abilità della sua comunità di hacker e il disprezzo per le forze dell'ordine occidentali. I migliori criminali informatici del mondo vivono in Russia e, poiché non viaggiano in paesi dove potrebbero essere arrestati, sono in gran parte immuni dall'azione penale. Ad esempio, uno dei criminali informatici che ha violato Yahoo per volere dei servizi dell'intelligence russi compromettendo milioni di account e trasferendo la PII

[16] Citati nel report "Economic impact of cybercrime" a cura del CSIS (Centro per gli studi strategici e internazionali) (Driggers, 2019)

(informazioni di identificazione personale) al governo russo, ha anche usato i dati rubati per spam e frodi di carte di credito a beneficio personale.
Fino a quando questi stati non cambieranno il loro comportamento interrompendo il supporto statale per l'hacking o applicando leggi contro l'hackeraggio criminale, il crimine informatico rimarrà un grave problema internazionale (Antonucci, 2017).

1.4. CHE COS'E' UN CYBER ATTACK?

Un cyber attack (o attacco informatico) è qualsiasi tentativo di esporre, alterare, disabilitare, distruggere, rubare o ottenere l'accesso non autorizzato a un sistema informatico, infrastruttura, rete o qualsiasi altro dispositivo intelligente (Hill, 2019).
In alcuni casi, gli attacchi informatici possono far parte di una guerra cibernetica o di sforzi terroristici, mentre altri crimini di questo tipo possono essere impiegati da individui, gruppi di attivisti, società o imprese. I tipi di attacchi informatici più frequenti e distruttivi verificatesi nel 2019 sono: Phishing, Formjacking, Cryptojacking, Ransomware e Man-in-the-middle attack.

1.4.1. PHISHING

Il phishing è un attacco informatico che maschera e-mail o siti internet per poi utilizzarli come arma con l'obiettivo di indurre la vittima a cliccare su un determinato collegamento o scaricare un particolare allegato, facendo credere che il messaggio sia legittimo, ad esempio una richiesta dalla banca o una nota di qualcuno in azienda.[17]
Il phishing è uno dei più antichi tipi di attacchi informatici, risalente agli anni '90, ed è ancora uno dei più diffusi e dannosi, con messaggi e tecniche sempre più sofisticati. "Phish" è pronunciato proprio come è scritto, vale a dire come la parola "fish" (pesce); l'analogia è quella di un pescatore che lancia un'esca (l'e-mail di phishing) e spera che qualcuno abbocchi.
Il termine è sorto a metà degli anni '90 tra gli hacker, il "ph" fa parte di una tradizione di ortografia stravagante ed è stato probabilmente influenzato dal termine "phreaking", abbreviazione di "phone freaking", una prima forma di hacking che implicava la

[17] www.cybersecurity360.it

riproduzione di toni sonori nei microtelefoni per ottenere telefonate gratuite. Quasi un terzo di tutte le violazioni nell'ultimo anno ha riguardato il phishing, invece per quanto riguarda gli attacchi di spionaggio informatico, quel numero passa al 78%[18]. La peggiore notizia del phishing per il 2019 è che i suoi autori stanno diventando molto più aggressivi a causa di strumenti e modelli ben realizzati e pronti all'uso.

Forse uno degli attacchi di phishing più famosi nella storia è accaduto nel 2016, quando gli hacker sono riusciti a convincere John Podesta, presidente della campagna di Hillary Clinton, a offrire la propria password di Gmail. L'attacco "fappening", in cui sono state rese pubbliche le foto intime di un certo numero di celebrità, era originariamente pensato come il risultato dell'insicurezza sui server iCloud di Apple, ma era in realtà il prodotto di numerosi tentativi di phishing che hanno avuto successo.

È possibile suddividere gli attacchi phishing in base allo scopo:

- l'invio di messaggi che mirano a indurre l'utente a rivelare dati importanti, spesso un nome utente e una password che vengono utilizzati successivamente per violare un sistema o un account.;
- invio di malware tramite e-mail di phishing che puntano a infettare il computer della vittima. malware è il ransomware: nel 2017 è stato stimato che il 93% delle e-mail di phishing conteneva allegati ransomware.

Paypal è in cima alla lista dei marchi più popolari utilizzati dagli hacker nei tentativi di phishing[19], in quanto brand finanziario con 250 milioni di conti attivi;

Figura 1.5: Top 5 brand utilizzati per il Phishing.

Fonte: Vade Secure report (Hadley, 2019).

[18] Secondo il Verizon Data Breach Investigation report (Vestberg, 2019).
[19] Stando al report "Phishers' favorites top 25" di Vade Secure (Hadley, 2019).

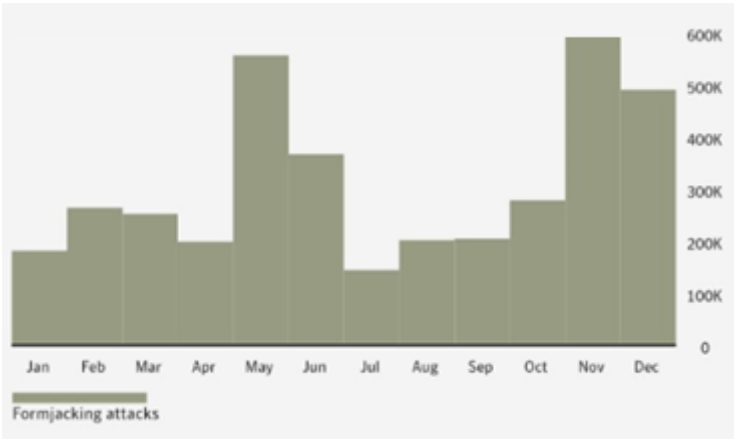
- si parla di Spear phishing quando gli aggressori tentano di creare un messaggio per attirare uno specifico individuo (un pescatore in questo caso punta un pesce specifico, piuttosto che lanciare un'esca nell'acqua.) I phisher identificano i loro obiettivi (a volte utilizzando informazioni su siti come LinkedIn) e usano indirizzi falsi per inviare e-mail che sembrano provenire da colleghi per cercare così di imbrogliare la preda.
- Il whale phishing, o caccia alle balene, è una forma di spear phishing rivolta ai pesci molto grandi: amministratori delegati, membri di consigli di amministrazione o altre figure che rivestono una certa autorità all'interno di un'impresa. Raccogliere informazioni sufficienti per ingannare un obiettivo di valore davvero elevato potrebbe richiedere del tempo, ma può avere un guadagno sorprendentemente alto.

1.4.2. FORMJACKING

Il formjacking è un tipo di attacco informatico in cui gli hacker inseriscono codici JavaScript pericolosi all'interno di un modulo di una determinata pagina Web, molto spesso una pagina di pagamento, in modo che, quando un visitatore inserisce i dati della propria carta di pagamento e invia i risultati, quel codice raccoglie il numero della carta di pagamento, nonché altre informazioni come il nome, l'indirizzo e il numero di telefono del cliente per poi inviarle a un'altra posizione a scelta degli aggressori[20].
Il formjacking fa parte di un gruppo più ampio di attacchi noti come "supply chain attack" in cui gli hacker prendono di mira un fornitore vulnerabile all'interno della catena di servizi/fornitura. Secondo la ricerca svolta da Symantec il formjacking nel 2018 ha mostrato una tendenza al rialzo con 4.818 siti Web compromessi con codici Javascript dannosi ogni mese (Hill, 2019)

[20] https://us.norton.com/internetsecurity-emerging-threats-what-is-formjacking.html.

Figura 1.6: Numero di attacchi formjacking avvenuti nel 2018.



Fonte: Symantec report (Hill, 2019).

Questa tendenza è sicuramente associabile agli enormi guadagni derivanti da questa pratica: i dati di una singola carta di credito vengono venduti fino a 40 euro sul dark web e con sole 10 carte di credito è possibile pervenire ad un rendimento massimo di 2 milioni di euro al mese (Antonucci, 2017).

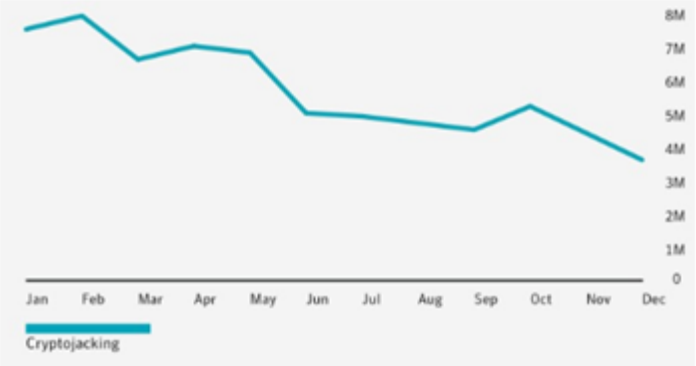
Questo è un problema globale con il potenziale di influenzare qualsiasi attività commerciale che, accetta pagamenti dai clienti online e la sua espansione potrebbe essere parzialmente spiegata dal calo di valore delle criptovalute: sussiste infatti la possibilità che i cybercriminali che utilizzavano i siti Web per il cryptojacking potrebbero ora optare per il formjacking.

1.4.3. CRYPTOJACKING

Il cryptojacking è una pratica in cui i criminali informatici, tramite i dispositivi delle vittime e a loro insaputa, usano il potere della loro CPU per estrarre le criptovalute. Questa attività di crittografia ha raggiunto il picco tra dicembre 2017 e febbraio 2018, con Symantec[21] che ha bloccato circa 8 milioni di eventi di crittografia al mese in quel periodo; tuttavia c'è stato un calo del 52% tra gennaio e dicembre 2018 molto probabilmente causato dallo stesso indebolimento prodotto dal bitcoin.

[21] Azienda leader globale in fatto di sicurezza informatica.

Figura 1.7: Distribuzione degli attacchi cryptojacking nel 2018.



Fonte: Symantec report (Hill, 2019).

La maggior parte dell'attività di crittografia ha continuato a provenire da coin miner basati su browser, dove l'estrazione di monete si svolge all'interno di una pagina Web, contenente uno script di mining e la potenza di calcolo dei visitatori della pagina Web verrà utilizzata per estrarre criptovaluta fino a quando quella stessa pagina rimarrà aperta. L'anonimato e le basse barriere all'ingresso hanno reso il cryptojacking talmente attraente consentendo ai criminali di superare il temporaneo (?) scoglio dato dal declino della criptovaluta, in modo tale di assumere un ruolo importante nel panorama della criminalità informatica[22].

1.4.4. RANSOMWARE

Il ransomware è una singolare forma di malware,[23] che rende inaccessibili i dati dei computer infettati e chiede un riscatto[24] sotto forma di pagamento per ripristinarli. Questi particolari virus hanno infatti come unico scopo l'estorsione di denaro per mezzo di "sequestro di file", attraverso la cifratura che, in pratica, rende il pc inutilizzabile. Al posto del classico sfondo vedremo comparire un avviso che sembra provenire dalla polizia o da un'altra organizzazione di sicurezza che, in cambio di una password in grado di sbloccare tutti i contenuti, intima di versare una somma di denaro abbastanza elevata (comunque quasi sempre sotto i 1.000 euro): generalmente la moneta usata è il bitcoin. Uno dei principali canali di diffusione sono i banner pubblicitari dei siti con contenuti per adulti,

[22] www.cybersecurity360.it
[23] Ransomware è appunto l'abbreviazione di malicious software.
[24] Ransom significa riscattare.

ma ci sono molti altri mezzi di cui si servono i criminali per trasmettere questa "infezione"[25]:

1. il più diffuso, perché purtroppo funziona molto bene, riguarda e-mail di phishing: attraverso questa tecnica, che sfrutta il social engineering vengono veicolati oltre il 75% dei ransomware;
2. la navigazione su siti compromessi: il cosiddetto "*drive-by download*" (letteralmente: download all'insaputa) da siti nei quali sono stati introdotti (da parte di hacker che sono riusciti a violare il sito) exploit kit che sfruttano vulnerabilità dei browser di Adobe Flash Player, Java o altri;
3. all'interno (in bundle) di altri software che vengono scaricati: per esempio programmi che ci promettono di "crackare" software costosi gratuitamente. È una pratica che oggi è diventata assai pericolosa, perché il crack che andremo a scaricare sarà un eseguibile (.exe), il quale potrebbe contenere una brutta sorpresa;
4. attacchi attraverso il desktop remoto[26]: sono attacchi con furto di credenziali (in genere di tipo "brute force") per accedere ai server e prenderne il controllo.

Il ransomware è il crimine informatico cresciuto in maniera più rapida, implica vari tipi di vittime: grandi aziende, piccole e medie imprese e singoli consumatori. Mentre il costo per l'individuo è basso, di solito circa 200 euro di riscatto, la capacità di colpire migliaia di bersagli a basso costo e senza rischio di penalità spiega perché questa categoria di criminalità informatica sta crescendo così rapidamente.

L'FBI riporta che 187 milioni sono il riscatto pagato nel primo trimestre del 2016 rispetto ai soli 24 milioni per tutto il 2015 (Lewis, 2018). Cosa ha provocato una crescita così esplosiva?

Il ransomware è iniziato anni fa con l'invio di floppy disk attraverso la posta, invitando le vittime a partecipare a un sondaggio per valutare il rischio di contrarre l'AIDS, però quando il disco è stato inserito, il suo software ha bloccato i computer e richiesto l'equivalente di 170 euro in contanti che dovevano essere spediti a Panama. Da allora è diventato molto più sofisticato.

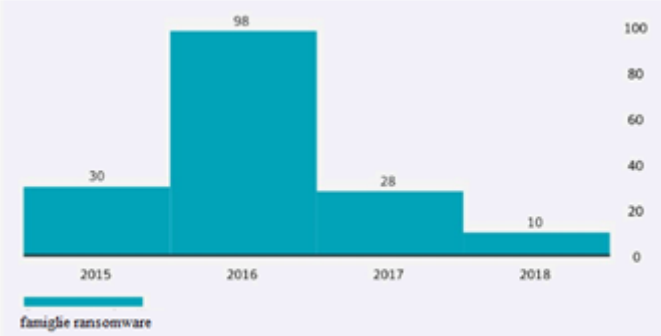
Dal 2012 al 2015, 33 nuove offerte di ransomware sono state rilasciate, ma quel numero è raddoppiato nel 2016 con 70 nuove famiglie di prodotti rese disponibili: stiamo

[25] www.cybersecurity360.it.

[26] RDP: remote desktop protocol, in genere sulla porta 3389.

assistendo alla commercializzazione di ransomware, disponibili online a partire da 2 euro fino a 3000 per specialisti (Ray et al., 2019)

Figura 1.8: Numero di nuove famiglie ransomware nate nel corso degli anni.



Fonte: Symantec report (Hill, 2019).

Con la rapidità con cui i kit guadagnarono popolarità, allo stesso modo iniziarono a essere sostituiti da Ransomware as-a-Service (RaaS) che consentirono agli autori dei programmi di ampliare notevolmente il loro potenziale, aprendo il proprio codice per l'uso e ottenendo così una percentuale dei riscatti risultanti.
La facilità d'uso è stato il principale motore della crescita del ransomware e, finché le vittime continuano a pagare, i criminali informatici continueranno ad affluire alle offerte di ransomware. Infine, si prevede che il ransomware aumenterà sempre di più sui sistemi mobili di destinazione, con i ransomware Android kit che stanno già iniziando ad apparire sui mercati.

1.4.5 MAN-IN-THE-MIDDLE ATTACK

Un attacco man-in-the-middle (tradotto letteralmente uomo nel mezzo) richiede tre giocatori: la vittima, l'entità con cui la vittima sta cercando di comunicare e "l'uomo nel mezzo", che sta intercettando le comunicazioni della vittima (Mallik et al., 2019). Fondamentale per lo scenario è che la vittima non sia a conoscenza dell'uomo nel mezzo. Un attacco MITM (Man In The Middle) tradizionale necessita l'accesso a un router Wi-Fi scarsamente protetto che solitamente si trova nelle aree pubbliche e persino nelle case di alcune persone. Le stesse prive di rete protetta, sono vittime di aggressori che possono eseguire la scansione del router alla ricerca di vulnerabilità specifiche come una password

debole. Sfruttate le debolezze del router, possono implementare strumenti per intercettare e leggere i dati trasmessi della vittima[27]. L'autore dell'attacco può quindi inserire i propri strumenti tra il computer della vittima e i siti Web visitati per acquisire credenziali di accesso, coordinate bancarie e altre informazioni personali.

[27] (AVG): https://www.avg.com/it/signal/man-in-the-middle-attack.

Capitolo 2

2. LE IMPRESE ACQUISISCONO CONSAPEVOLEZZA DEL PROBLEMA

2.1. LA NECESSITÀ DI INVESTIRE IN SICUREZZA INFORMATICA

Il bisogno di innovazione, la spinta verso migliori prestazioni e lo sfruttamento di nuove tecnologie possono realisticamente verificarsi solo includendo la sicurezza informatica nel business, invece di affrontarla come ripensamento.

Anche se molte organizzazioni continuano a considerare la cybersecurity come un problema tecnico, si iniziano a notare i primi cambiamenti, destinati a migliorare l'efficacia della gestione del rischio informatico. La sicurezza informatica viene sempre più considerata un attivatore per il business delle imprese: la cyber security deve diventare una capacità organizzativa di base che coinvolge tutti i dipartimenti e non solo la tecnologia dell'informazione (IT)[28]; infatti la maggior parte dei consigli di amministrazione (82%) si dimostra preoccupata per la sicurezza informatica e ciò dovrebbe tradursi in azione.

Una probabile conseguenza dell'attenzione della dirigenza riguarda l'aumento del 61% del budget destinato alla cyber security, l'allineamento della strategia informatica agli obiettivi aziendali, lo sviluppo e il rispetto delle politiche informatiche da parte della maggioranza delle organizzazioni (66%).

Collegare le attività informatiche agli obiettivi e aspirazioni aziendali è forse l'elemento più importante per diventare un'impresa gestita dal rischio informatico. Il cyber diventa parte integrante dello sviluppo di nuovi prodotti, servizi e capacità; gli investimenti sono necessari per tenere il passo con le minacce informatiche. I finanziamenti aggiuntivi forniranno quindi una maggiore compensazione per specialisti informatici qualificati, una formazione più efficace, attività di sensibilizzazione più ampie e una pianificazione più proficua di risposta e recupero (Antonucci, 2017).

[28] Informazione emersa dalla ricerca congiunta di RSA Conference e ISACA (Downs, 2019).

2.2. SVILUPPO DELLA GESTIONE DEL RISCHIO INFORMATICO

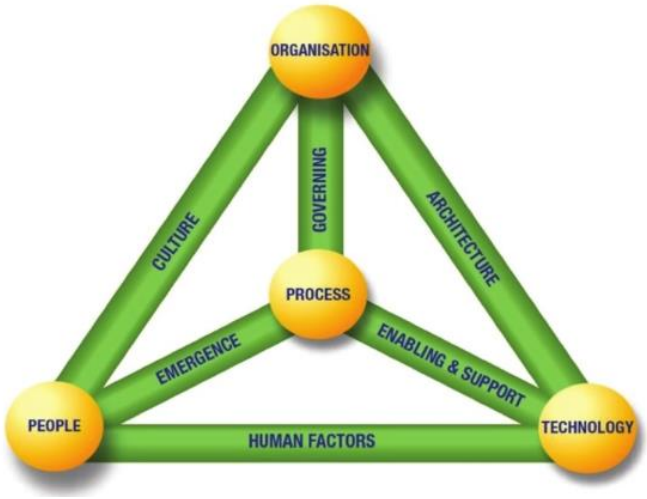
Le organizzazioni con migliori prestazioni e capacità di gestione dei rischi informatici più mature, condividono diverse caratteristiche (van Kessel, 2019):

- riconoscono l'importanza della sicurezza informatica e la affrontano come problema del consiglio di amministrazione e promotore del valore;
- assicurano che il management esecutivo si impegni a guidare gli sforzi informatici e sostengono la cyber security come un problema aziendale;
- gestiscono i cyber risk nell'ambito di un approccio di gestione dei rischi aziendali fornendo il supporto umano e di capitale per programmi e iniziative;
- seguono i manager di sicurezza informatica consolidati nella costruzione, gestione e monitoraggio del programma informatico aziendale;
- valutano continuamente le prestazioni di sicurezza informatica rispetto agli obiettivi aziendali;
- tengono traccia e segnalano le prestazioni di sicurezza informatica rispetto agli standard internazionali utilizzati per progettare e attuare il programma;
- perfezionano le priorità e le attività di cyber sicurezza man mano che le esigenze e le minacce delle imprese cambiano.

Ciò che distingue le organizzazioni con le migliori prestazioni consiste nell’affrontare la sicurezza informatica come parte integrante del business, che coinvolge tutti, dal consiglio di amministrazione ai semplici utenti; infatti le migliori imprese in genere subiscono meno incidenti, il loro impatto è meno grave e i tempi di recupero sono più rapidi (Singer, 2014).

Raggiungere tale livello di preparazione e difesa informatica si è rivelato una sfida; da allora i leader aziendali, che dovevano comprendere il proprio ruolo, non avevano a disposizione una guida orientata al business. L'informazione e la sicurezza informatica sono apparse come un problema tecnico e non un elemento fondamentale sulle attività di procedura e sulle modalità in cui l'azienda opera. Il valore è stato interpretato come proveniente da nuovi prodotti o dall'adozione di nuove tecnologie, senza collegare la necessità di protezione con strategie di business a valore aggiunto (Craigen et al., 2014).

Figura 2.1: Concettualizzare la sicurezza informatica all'interno dell'impresa.



Fonte: The Cyber Risk Handbook (Antonucci, 2017).

Questa figura raccoglie gli elementi essenziali presenti in ogni organizzazione e l'interconnessione degli stessi: ogni impresa può essere descritta in termini di struttura organizzativa, persone, tecnologia utilizzata e processi che, uniscono la triade per raggiungere gli obiettivi aziendali; ciò che viene trascurato è l'importanza della cultura che collega le persone all'interno dell'organizzazione. Il fattore umano è molto rilevante per rendere la tecnologia utile sia per i clienti, che per il personale e il design tecnologico ha il compito di essere efficace nel supportare il business.

Spesso nelle guide di riferimento per professionisti della sicurezza informatica e leader aziendali è assente il potere abilitante della governance, che collega la progettazione dell'organizzazione ai processi, quali la tecnologia deve promuovere processi più efficaci, i quali supportino l'abilitazione aziendale attraverso la tecnologia. La comprensione della sicurezza informatica, come parte di un sistema, indirizzerà il consiglio e il management a una migliore comprensione della cyber defence all'interno dell'organizzazione e dei suoi componenti, che devono essere attivati per creare la cultura, le strutture e i programmi necessari per un'efficace sistema di gestione del rischio (Jang-Jaccard, 2014).

Nella pianificazione e nell'esecuzione di attacchi contro le imprese, gli hacker adottano spesso un approccio olistico, considerandolo come miglior modo per superare le difese, che le organizzazioni hanno costruito per proteggere le informazioni commerciali, i dati sensibili e le risorse critiche. Gli aggressori imboccano le strade che presentano debolezze comprendendo che la cultura e il comportamento dell'organizzazione, oltre ai servizi e

alle applicazioni, possono rivelarsi facili percorsi di accesso per un compromesso, anziché difese competenti.

La creazione di persuasivi messaggi di posta elettronica ha lo scopo di invogliare gli utenti ad aprire un allegato, visitare un sito Web infetto o a divulgare le credenziali di sicurezza in risposta a un messaggio forzato da parte del supporto tecnico e rappresentano meccanismi efficaci di attacco frequente (Jang-Jaccard, 2014).

Un'organizzazione matura gestita dal rischio crea consapevolezza del fatto che i messaggi apparentemente legittimi non dovrebbero essere considerati attendibili quando contrastano con i processi stabiliti e laddove la cultura dell'impresa sostiene l'idea che sia accettabile mettere in discussione la legittimità di una richiesta (Compare, 2019).

Il 21 ° EY Global Information Security Survey (GISS) esplora le più importanti questioni di cyber sicurezza che le organizzazioni affrontano, cercando di individuare da oltre vent'anni la loro consapevolezza a proposito della crescente minaccia del cyber crime e quindi la necessità di affrontare questo problema alla radice con una certa urgenza (van Kessel, 2019).

Gli attacchi continuano a crescere sia per numero che per raffinatezza, la gamma di hacker si sta espandendo, l'innovazione digitale e le nuove tecnologie stanno esponendo le società a nuove vulnerabilità.

Quest'anno l'analisi EY delle risposte dei CIO, CISO e altri dirigenti mostra che molte imprese stanno incrementando le risorse dedicate alla sicurezza informatica, ma anche testimoniano le loro preoccupazioni per la portata e la gravità della minaccia (van Kessel, 2019).

I rischi informatici si stanno evolvendo; qualsiasi organizzazione che si consideri al riparo da un attacco informatico rischia di dover subire uno shock, inoltre l'obiettivo comune dovrebbe essere non solo proteggere l'impresa con una buona conoscenza sulla cyber sicurezza e sulle linee base di difesa, ma anche ottimizzare la risposta con strumenti e strategie avanzati (Craigen et al., 2014).

La cyber security deve necessariamente presentarsi in qualità di funzione abilitante, piuttosto che un blocco per l'innovazione e il cambiamento; per il 2019 si è deciso[29] di esplorare questi temi in modo più dettagliato, condividendo le idee e le pratiche guida per migliorare la sicurezza informatica di chiunque.

[29] La ricerca ISACA e il GISS si sono spostati verso questi temi.

Le imprese investono di più sulla la sicurezza informatica, dedicando risorse crescenti al miglioramento delle proprie difese e impregnandosi per integrare la sicurezza in base alla progettazione, ma i risultati del sondaggio suggeriscono che tutto ciò è insufficiente: oltre i tre quarti (87%) delle imprese non dispongono di un budget tale da garantire i livelli richiesti per la sicurezza informatica e resilienza desiderate; le protezioni sono frammentarie, poche organizzazioni stanno dando la priorità alle capacità avanzate e troppo spesso la cybersecurity rimane taciuta o isolata. La sfida per le organizzazioni è quella di progredire su tre fronti (van Kessel, 2019):

- proteggere l'azienda, quindi concentrarsi sull'identificazione delle risorse e sulla costruzione di linee di difesa, il futuro della sicurezza informatica;
- ottimizzare la sicurezza informatica, perciò focalizzarsi sull'arresto delle attività di basso valore, sull'aumento dell'efficienza e sul reinvestimento dei fondi in tecnologie emergenti e innovative per migliorare la protezione esistente;
- consentire la crescita quindi indirizzarsi sull'implementazione della sicurezza secondo la progettazione, come fattore chiave di successo per le innovazioni digitali.

Questi tre imperativi devono essere perseguiti contemporaneamente, anche se la frequenza e la portata delle violazioni della sicurezza in tutto il mondo mostrano che pochissime imprese hanno implementato persino il livello base. Tuttavia, anche se cercano di recuperare, le società devono andare avanti perfezionando le difese esistenti per ottimizzare la sicurezza e supportare la crescita (Lewis, 2018).

Figura 2.2: Dati preoccupanti relativi al 2018 emersi dalla ricerca di EY Global Information Security Survey (2018).

Fonte: EY Global Information Security Survey (van Kessel, 2019).

L'analisi di ISACA evidenzia un numero significativo (77%) di imprese che opera ancora con limitata sicurezza informatica e resilienza; esse infatti potrebbero anche non avere un quadro chiaro di quali e dove siano le loro informazioni e risorse più critiche, né disporre di garanzie adeguate a proteggere tali risorse (Downs, 2019); pertanto è importante che la maggior parte di esse continui a concentrarsi sulle basi.

Dovrebbero prima identificare i dati chiave e la proprietà intellettuale (i "gioielli della corona"), quindi rivedere le capacità di sicurezza informatica, i processi di gestione degli accessi e infine aggiornare lo scudo di protezione.

Le domande che le imprese devono inevitabilmente porsi sono (Singer, 2014):

- Quali sono le nostre risorse di informazione più preziose?
- Dove sono i nostri punti deboli in fatto di cyber sicurezza?
- Quali sono le minacce che stiamo affrontando?
- Chi sono i potenziali protagonisti di tali minacce?
- Siamo già stati violati o compromessi?
- In che modo la nostra protezione si confronta con la concorrenza?
- Quali sono le nostre responsabilità normative, le stiamo rispettando?

È necessario esaminare dapprima le quattro componenti vitali della protezione dell'impresa (Lewis, 2018):

1. Governance. Le organizzazioni dovrebbero affrontare la misura in cui la sicurezza informatica è parte integrante della strategia dell'organizzazione e se vi sono fondi sufficienti per gli investimenti necessari nella difesa.
2. Qual è il rischio? Cosa temono di più le organizzazioni e come considerano le maggiori minacce da affrontare?
3. Protezione. La maturità della sicurezza informatica di un'impresa e le vulnerabilità più comuni sono fondamentali.
4. Violazioni. Il modo in cui vengono identificate le violazioni e il modo in cui le organizzazioni rispondono sono questioni critiche.

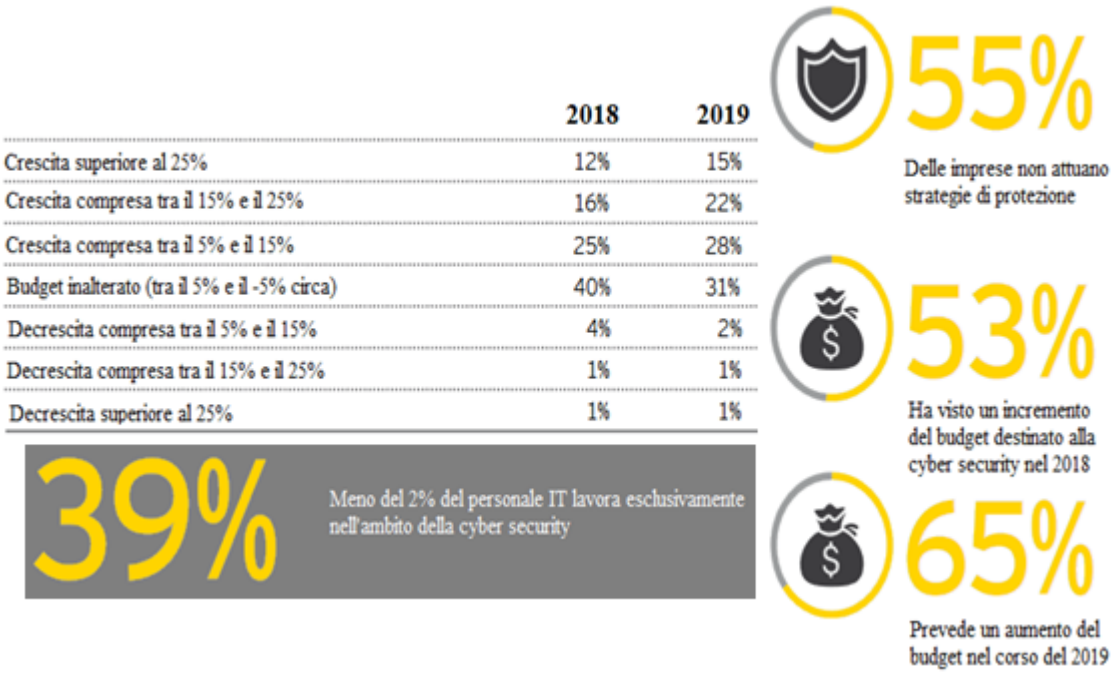
Un problema generale si riscontra nella carenza di competenze: le stime identificano una carenza globale di circa 1,8 milioni di professionisti della sicurezza entro cinque anni. Anche nei settori più dotati di risorse, le organizzazioni stanno lottando per reclutare gli esperti di cui hanno bisogno e i servizi finanziari ne sono un esempio.
Come afferma Jeremy Pizzala (2017), leader della sicurezza informatica della EY Global Services, "è indispensabile attirare più donne e minoranze nella forza lavoro della cyber sicurezza sia per aumentare i numeri che per costruire una risorsa in grado di contrastare la minaccia, poiché la diversità è un imperativo commerciale". Diversi team ottengono risultati migliori in tutta l'impresa essendo più innovativi, obiettivi e collaborativi e questo è fondamentale nella sicurezza informatica, dove ogni giorno si combatte per stare un passo avanti rispetto agli aggressori ".

2.2.1. GOVERNANCE: LA SICUREZZA INFORMATICA FA PARTE DELLA STRATEGIA, È COMPRESA NEL BUDGET?

Dato l'incremento dell'innovazione digitale, è necessario un budget più elevato destinato alla sicurezza informatica (von Solms, 2018). Quasi tutte le aziende guardano alle tecnologie come la robotica, l'apprendimento automatico, l'intelligenza artificiale, la blockchain e così via; in ogni caso tutto questo cambiamento arriverà con ulteriori rischi informatici e investimenti necessari. "Più della metà delle imprese non fa della protezione parte integrante della strategia e dei piani di esecuzione". Sorprendentemente, **le**

organizzazioni più grandi hanno maggiori probabilità di non essere all'altezza rispetto alle organizzazioni più piccole (58% contro 54%), la buona notizia è che i budget per la sicurezza informatica sono in aumento, tuttavia, le aziende più grandi hanno maggiori probabilità di aumentare i budget quest'anno (63%) e nel prossimo (67%) rispetto alle società più piccole (50% e 66%) (van Kessel, 2019).

Figura 2.3: Cambiamento del budget destinato alla sicurezza informatica per l'anno 2018.



Fonte: EY Global Information Security Survey (van Kessel, 2019).

2.2.2. QUAL È LA POSTA IN GIOCO, QUALE LA PAURA PIÙ GRANDE E QUALI SONO LE MAGGIORI MINACCE?

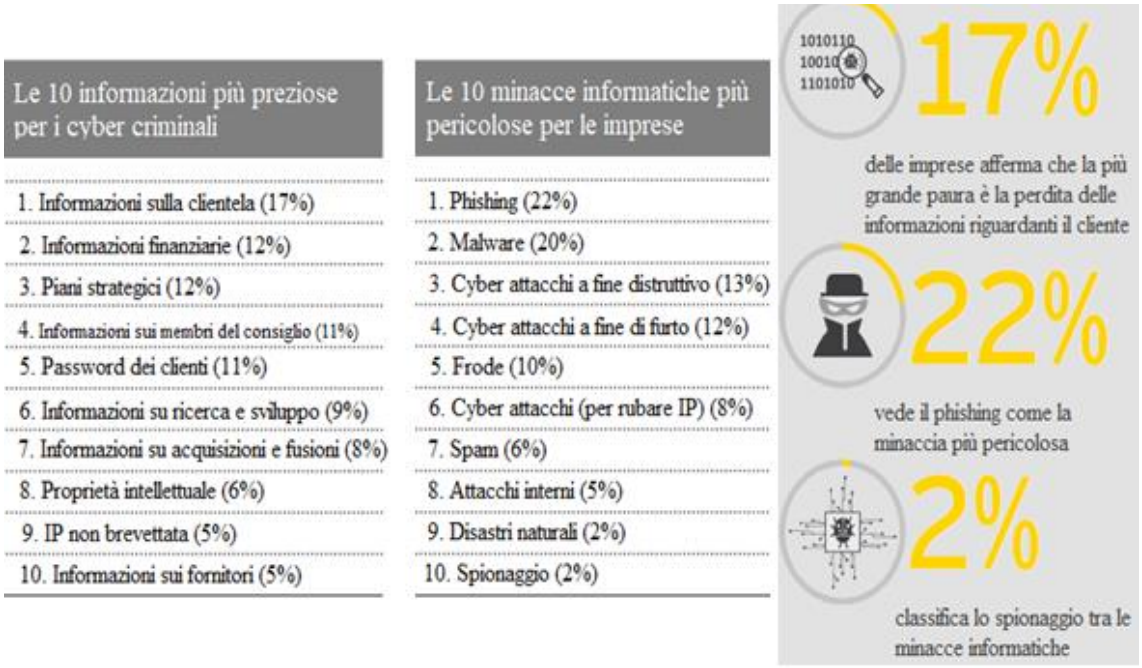
È importante sottolineare che sempre più imprese stanno iniziando a riconoscere l'ampia natura della minaccia, infatti il lato positivo del 2019, in parte a causa di alcuni di alcuni grandi attacchi informatici a cui abbiamo assistito a livello globale, è la crescente consapevolezza che la sicurezza riguarda anche il mantenimento della continuità delle operazioni aziendali e non solo sulla sicurezza dei dati e della privacy (Singer, 2014).
Qual è la cosa più preziosa? Non sorprende che i dati sulla clientela, le informazioni finanziarie e i piani strategici costituiscano le prime tre informazioni più preziose da proteggere. Tra i dati sensibili troviamo inoltre quelli relativi ai membri del board e le

password dei clienti, oltre alle informazioni sui fornitori che stanno a dimostrare l'ambizione di proteggere l'intera catena di approvvigionamento. Tutto ciò necessita comunque di un ulteriore lavoro.

Quali sono le maggiori minacce? La maggior parte delle violazioni informatiche di successo contengono "phishing e /o malware "come punti di partenza seguite da attacchi di disturbo e assalti incentrati sul furto di denaro (Jang-Jaccard, 2014).

Sebbene ci siano state molte discussioni sulle minacce interne e sulle offensive sponsorizzate dallo stato, la paura di questi attacchi si manifesta al numero otto sulla lista con lo spionaggio collocato in fondo all'elenco.

Figura 2.4: Le 10 informazioni più preziose e le 10 minacce più pericolose.



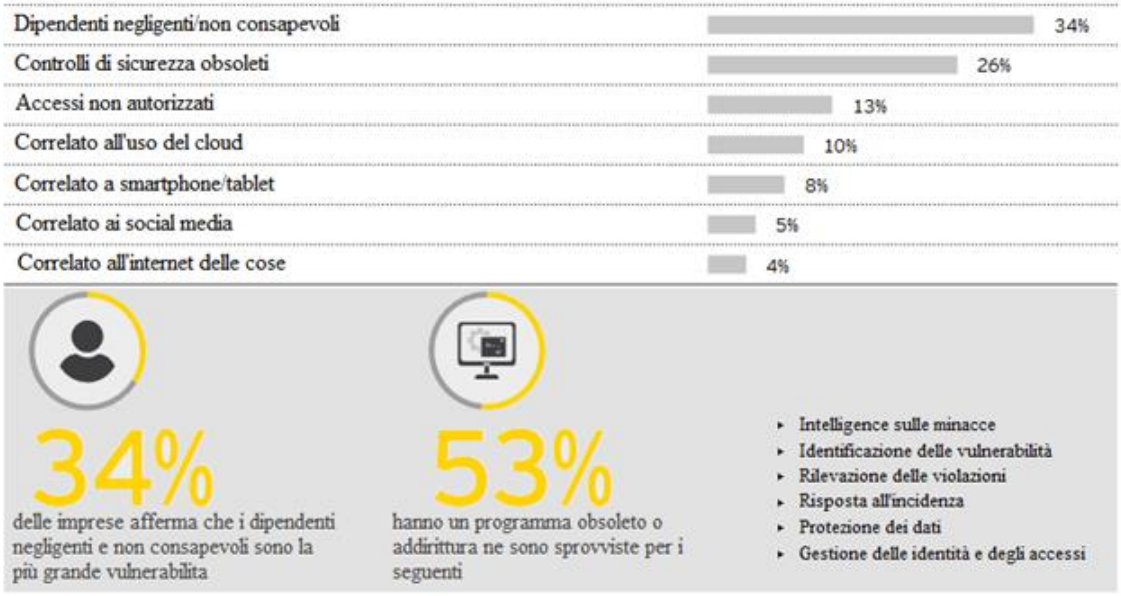
Fonte: EY Global Information Security Survey (Van Kessel, 2019).

2.2.3. PROTEZIONE: QUALI SONO LE VULNERABILITA' PIU' RISCHIOSE E QUANTO È MATURA LA SICUREZZA INFORMATICA?

Sono necessari diversi mesi per captare attacchi sofisticati. La sfida in questo ambito è la difficoltà nell'identificare gli efficaci strumenti di individuazione e verifica delle minacce: le organizzazioni lottano confrontandosi sulla soluzione ottimale. Di conseguenza, relativamente poche imprese hanno "implementato qualsiasi cosa" (Jang-Jaccard, 2014).

Le vulnerabilità aumentano quando si tratta di terze parti, infatti solo il 15% delle organizzazioni ha adottato misure protettive di base contro le minacce provenienti da terze parti; il 36% è a conoscenza dei rischi attraverso autovalutazioni (22%) o valutazioni indipendenti (14%); pertanto, il 64% non è a conoscenza del problema (tra le aziende più piccole, questo dato sale al 67%). Le società più grandi sono più mature delle loro controparti più piccole, ad esempio il 35% dispone di un programma di intelligence forte e aggiornato relativamente alle minacce informatiche, rispetto al 25% delle organizzazioni più piccole e il 58% afferma che il programma di risposta agli incidenti è aggiornato, rispetto al 41% delle piccole imprese (Downs, 2019).

Figura 2.5: Le vulnerabilità con l'esposizione al rischio più elevata nel corso degli ultimi 12 mesi.



Fonte: EY Global Information Security Survey (Van Kessel, 2019).

2.2.4. VIOLAZIONI: COME VENGONO IDENTIFICATE E COME NE RISPONDONO LE IMPRESE?

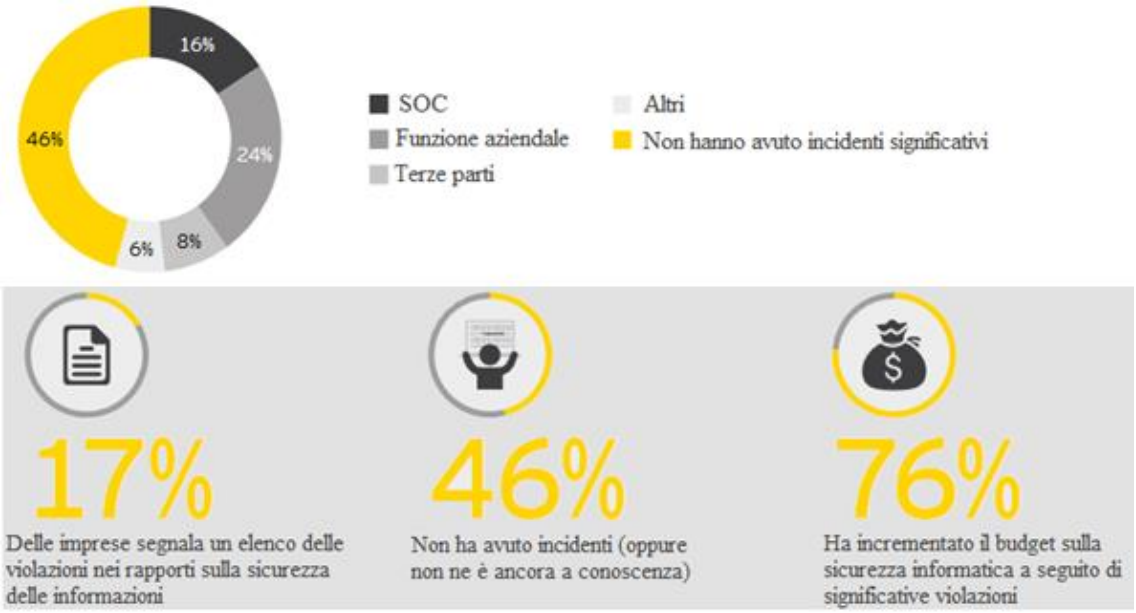
Le aziende veramente intelligenti e lungimiranti ora hanno due budget: quello tradizionale e quello di emergenza per eventualità impreviste quali l'affiorare di un nuovo tipo di minaccia, violazione o compromesso (Compare, 2019).

Le organizzazioni ammettono che sarebbe improbabile l'intensificazione delle loro pratiche di sicurezza informatica o l'incremento della spesa a meno che esse non abbiano

subito una sorta di violazione o incidente che ha causato impatti molto negativi. Una violazione in cui non è stato riscontrato alcun danno non porterebbe ad una spesa maggiore per il 63% delle organizzazioni[30].

Molte imprese non sono chiare sull'identificazione di violazioni o incidenti e, tra le organizzazioni che sono state colpite da questi nell'ultimo anno, meno di un terzo afferma che grazie al centro di sicurezza vi è stato riscontro della violazione.

Figura 2.6: Da chi vengono scoperte le violazioni?



Fonte: EY Global Information Security Survey (Van Kessel, 2019).

2.3. COSA SIGNIFICA "CYBER SECURITY"?

La cyber security, o sicurezza informatica, si riferisce generalmente alla capacità di controllare l'accesso ai sistemi di rete e alle informazioni in essi contenute[31].

Laddove i controlli di sicurezza informatica si rivelano efficaci, il cyber spazio è considerato un'infrastruttura digitale affidabile e resistente, ma, laddove i controlli di sicurezza informatica sono assenti, incompleti o mal progettati, esso viene considerato il selvaggio west dell'era digitale.

[30] Nella maggior parte dei casi è stato fatto un danno ma esso non è ancora apparso in superficie.
[31] www.cybersecurity360.it

Generalmente la sicurezza informatica viene in genere spiegata in termini di alcune triadi che descrivono gli obiettivi dei professionisti della sicurezza e i loro metodi (Bayuk 2010). Alcune triadi si combinano al fine di coprire la maggior parte degli usi del termine che sono:

- prevenire, rilevare, rispondere;
- persone, processo, tecnologia;
- riservatezza, integrità e disponibilità.

Tradizionalmente, l'obiettivo principale della pianificazione della sicurezza riguarda la prevenzione di un attacco avversario riuscito, tuttavia, tutti i professionisti della sicurezza sono consapevoli del fatto che non è semplicemente possibile prevenire tutti gli attacchi, quindi la pianificazione e la preparazione devono includere anche metodi per rilevare gli attacchi in corso, preferibilmente prima che possano causare danni (Antonucci, 2017).
Ciò nonostante, indipendentemente dal fatto che i processi di rilevamento siano efficaci o meno, una volta reso evidente che un sistema sia stato minacciato, la sicurezza include la competenza di rispondere a tali incidenti.
Nella sicurezza informatica, il terzo elemento della triade è spesso dichiarato in una forma leggermente più ottimistica, infatti, piuttosto che "rispondere", si tratta di "recuperare" o "correggere", poiché i professionisti hanno l'aspettativa che i danni possano essere completamente eliminati.
La triade "persone, i processi e la tecnologia" se applicata alla cyber security, evidenzia il fatto che essa non è raggiunta dai soli professionisti e che la sicurezza informatica non può essere realizzata solo con la tecnologia, ma riconosce che il sistema o l'organizzazione da proteggere include altri elementi umani le cui decisioni e azioni svolgono un ruolo vitale nel successo dei programmi di sicurezza.
Le persone implicate presentano motivazioni e interessi diversi e si comportano in modo sicuro individualmente, non saprebbero come agire a livello collettivo per prevenire, rilevare e recuperare dai danni senza un processo pianificato; pertanto i professionisti della sicurezza dovrebbero integrare i programmi di sicurezza nei processi organizzativi esistenti e fare un uso strategico della tecnologia a supporto degli obiettivi di sicurezza informatica.
Riservatezza, integrità e disponibilità riguardano gli obiettivi di sicurezza specifici delle informazioni. La riservatezza si riferisce alla capacità di un sistema di limitare la diffusione delle informazioni all'uso autorizzato, l'integrità è la capacità di mantenere

l'autenticità, mentre la disponibilità si riferisce alla consegna tempestiva della capacità funzionale.
Questi obiettivi di sicurezza delle informazioni si applicavano alle informazioni anche prima che queste fossero sui computer, ma l'avvento del cyberspazio ha cambiato i metodi con cui gli obiettivi sono stati raggiunti, così come una certa difficoltà a ottenerli. Le tecnologie a supporto della riservatezza, integrità e disponibilità sono spesso in contrasto tra loro; ad esempio, gli sforzi per raggiungere un elevato livello di disponibilità di informazioni nel cyber spazio rendono spesso più difficile mantenere la riservatezza delle informazioni.
Il compito del professionista della sicurezza informatica è appunto prevenire, rilevare e recuperare danni alla riservatezza, all'integrità e alla disponibilità delle informazioni nel cyber spazio (Compare, 2019).

2.3.1. LA CYBER SECURITY NEL SETTORE SANITARIO

Il settore sanitario deve immagazzinare quantità crescenti di informazioni personali identificabili e sensibili.
Il GISS (global information security survey) del 2019 suggerisce che la consapevolezza verso i rischi informatici sta aumentando e molte organizzazioni sono determinate a rafforzarsi, tuttavia è necessario uno sforzo maggiore (Van Kessel, 2019). Questo settore ha subito una serie di incidenti informatici negli ultimi mesi; in un caso particolare, un bug nella sicurezza in uno dei più utilizzati sistemi di gestione del paziente, ha messo a repentaglio quasi 100 milioni di dati. In un'altra circostanza sono state esposte al rischio informazioni quali il nome, la data di nascita, l'assicurazione, lo stato di disabilità e l'indirizzo di casa di 2 milioni di pazienti in America Centrale.
I dati sanitari sono estremamente preziosi sul "dark web", pertanto le organizzazioni sanitarie risultano attraenti per gli aggressori.
Un'impresa sanitaria su tre in America ha subito un attacco informatico, e 1 su 10 è stata costretta a versare un riscatto (Kruse et al., 2017).
La situazione attuale nel settore sanitario:

- governance. La metà delle imprese sanitarie, governative e del settore pubblico affermano di aver aumentato la spesa destinata alla sicurezza informatica per l'anno 2018, mentre il 66% prevede di aumentare tale spesa per l'anno successivo.

- Qual è il rischio? Il 17% delle aziende del settore sanitario afferma che le informazioni personali della clientela sono molto preziose per i criminali informatici, mentre il 25% confessa di sentirsi più esposto al rischio di virus e malware.
- Protezione. I dipendenti negligenti o inconsapevoli vengono visti dal 33% delle aziende sanitarie come la vulnerabilità che ha causato un aumento dell'esposizione al rischio per il 2018.
- Violazioni. Solo il 18% delle imprese sanitarie si sente fiducioso nel rilevare un attacco informatico.

2.3.2. LA CYBER SECURITY NEL SETTORE ENERGETICO

Il settore energetico ha beneficiato di tecnologie emergenti sempre più sofisticate, ma questo significa che si sta rendendo maggiormente vulnerabile a livello informatico e operativo (van Kessel, 2019). Attacchi di successo verso questo settore possono avere conseguenze devastanti, privando potere alle comunità e persino mettendo a repentaglio la sicurezza dei cittadini. Ci sono molte prove a dimostrazione del fatto che le compagnie energetiche sono finite sul radar dei cyber criminali; infatti in un recente caso, i ricercatori della sicurezza hanno scoperto il tentativo di infiltrazione di hacker russi nelle imprese degli Stati Uniti e in un'altra circostanza le società elettriche sono state colpite da truffe phishing provenienti dalla Corea del Nord. La minaccia ha spinto i regolatori in Europa e altrove a esaminare nuove norme per incoraggiare il settore a proteggere le imprese.
La situazione attuale nel settore energetico:

- Governance. Oltre la metà (57%) delle aziende energetiche ha aumentato la spesa destinata alla cyber security per il 2018 e il 68% prevede di incrementare questa spesa per il 2019.
- Qual è il rischio? Il 15% delle aziende del settore considera i dati personali dei clienti come materiale più prezioso per il cyber crime, mentre il 14% considera i piani strategici come dato più prezioso. Il 27% afferma di essere seriamente esposto nei confronti del phishing.
- Protezione. Circa 3 imprese energetiche su 10 (29%) affermano che i dipendenti negligenti o inconsapevoli rappresentano il tipo di vulnerabilità più rilevante. La

stessa proporzione (28%) cita invece i controlli o l'architettura delle informazioni come obsoleti.

- Violazioni. Più di 4 aziende su 10 (42%) affermano di non aver avuto un incidente significativo sulla sicurezza informatica nel corso del 2018.

2.4. OTTIMIZZARE LA SICUREZZA INFORMATICA

Il GISS di quest'anno suggerisce che il 77% delle organizzazioni sta ora cercando di andare oltre la messa in atto di protezioni di sicurezza informatica di base per perfezionare le proprie capacità (Van Kessel, 2019).
Le domande che le imprese devono porsi:

- qual è la nostra strategia di sicurezza informatica e quali sono i "gioielli della corona"?
- Qual è la tolleranza e appetito per il rischio?
- Esistono attività di basso valore che si potrebbe svolgere in modo più rapido o economico?
- In che modo potrebbero essere d'aiuto le tecnologie come l'automazione dei processi robotici, l'intelligenza artificiale e gli strumenti di analisi dei dati?
- Dove si dovrebbero rafforzare ulteriormente le proprie capacità?
- Cosa si potrebbe smettere di fare e come si potrebbero investire le risorse liberate?

Parte di questo sforzo viene svolto considerando e implementando l'intelligenza artificiale, robotica e di analisi per aumentare la sicurezza dei propri beni e dati chiave anche se, al momento, esiste un notevole margine di miglioramento.
Meno di 1 impresa su 10 afferma che la funzione di sicurezza delle informazioni attualmente soddisfa pienamente le esigenze e molti sono preoccupati dai miglioramenti che non sono ancora in corso. È più probabile che piccole aziende siano in ritardo: il 78% delle organizzazioni più grandi afferma che la funzione di sicurezza delle informazioni sta soddisfacendo almeno in parte le esigenze, percentuale ridotta al 65% per le controparti più piccole (Downs, 2019).
I criminali informatici stanno aumentando il loro gioco e il prezzo del fallimento è alto. In un recente attacco, una banca indiana ha perso 944 milioni di rupie (12 milioni di euro),

dopo che gli hacker hanno installato malware sul loro server ATM, permettendo di effettuare prelievi fraudolenti dai bancomat.

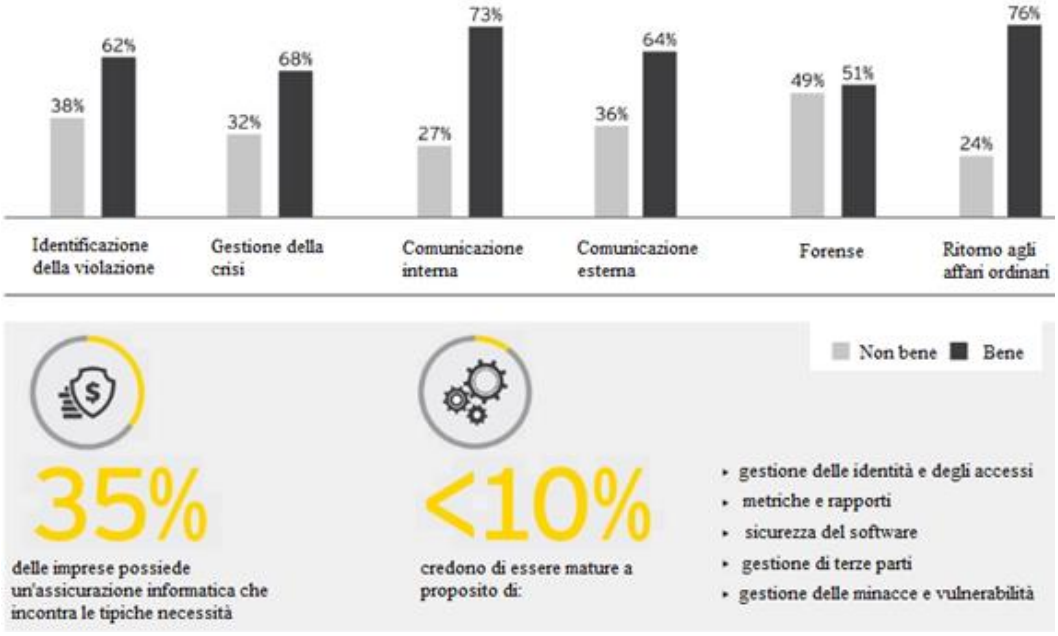
2.4.1. LA SITUAZIONE ATTUALE: LA FUNZIONE DI SICUREZZA DELLE INFORMAZIONI SODDISFA LE ESIGENZE DELL'IMPRESA?

Quanto è grave il deficit?

Complessivamente, il 92% delle imprese è preoccupato per la propria funzione di sicurezza delle informazioni nei settori chiave. Le aziende più piccole sono particolarmente preoccupate: il 28% afferma che la propria funzione di sicurezza delle informazioni non soddisfa attualmente le esigenze o deve essere migliorata e il 56% dichiara di avere carenze di competenze o vincoli di bilancio (van Kessel, 2019).

Una migliore pianificazione ed esecuzione della risposta agli incidenti è un'area importante, in cui sempre più imprese devono ottimizzare le proprie capacità. La medicina legale è una particolare area di debolezza e questo mina la capacità delle organizzazioni di capire cosa sia andato storto e migliorare il livello di protezione. Le aziende più piccole sono particolarmente preoccupate: il 39% mostra fragilità nell'identificare le violazioni e il 52% è turbato dalle proprie capacità forensi.

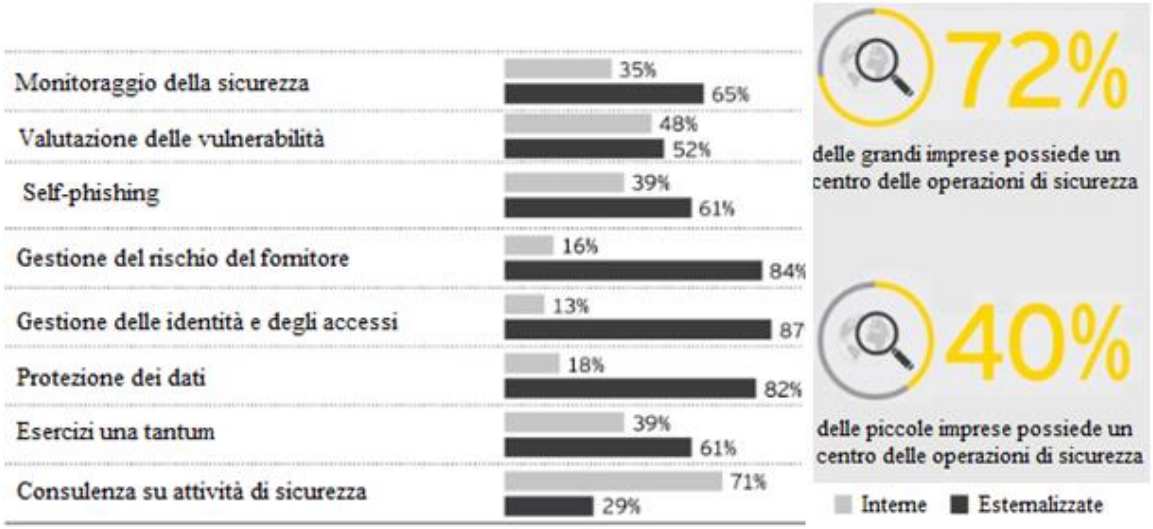
Figura 2.7: Come si comportano le imprese con le priorità da migliorare in caso di violazione?



Fonte: EY Global Information Security Survey (van Kessel, 2019).

In che modo le organizzazioni migliorano rapidamente le proprie capacità, cosa dovrebbero fare internamente e dove conviene cercare un supporto esterno? Le maggiori società finanziarie hanno introdotto centri di "fusione" che combinano le capacità di sicurezza informatica con molteplici altre competenze, come i sistemi utilizzati per il riciclaggio di denaro sporco e per conoscere i propri clienti.

Figura 2.8: Quali informazioni vengono eseguite internamente e quali esternalizzate?



Fonte: EY Global Information Security Survey (van Kessel, 2019).

L'interesse nei rapporti sulla sicurezza informatica a livello di consiglio è cresciuto dai tentativi di comprendere la tecnologia al punto in cui il board aziendale ha ora la responsabilità fiduciaria di gestire il rischio di cyber sicurezza. Amministratori, azionisti e regolatori stanno facendo pressioni per una migliore comunicazione, anche se le imprese non si stanno ancora muovendo verso una posizione di divulgazione esterna (Singer, 2014).

Solo il 15% delle organizzazioni afferma che i report sulla sicurezza delle informazioni attualmente soddisfano pienamente le aspettative, mentre le aziende più piccole dovranno aggiornarsi rapidamente: quasi un quarto (23%) attualmente non produce report sulla sicurezza delle informazioni, rispetto al 16% delle organizzazioni più grandi.

2.5. INCENTIVARE LA CRESCITA: COME RENDERE LA SICUREZZA INFORMATICA PARTE DELLA STRATEGIA?

Le imprese stanno attraversando un processo di trasformazione digitale la cui natura varia a seconda del tipo di organizzazione, ma avrà almeno una o più delle seguenti componenti: vendita/supporto online ai clienti, integrazioni della catena di fornitura, applicazione dell'automazione dei processi robotici, intelligenza artificiale, blockchain e analisi, modello di business e innovazione sul posto di lavoro (van Kessel, 2019).
Le organizzazioni sono ora convinte che la cura del rischio informatico e la costruzione della sicurezza sin dall'inizio siano indispensabili per il successo nell'era digitale. L'attenzione ora dovrebbe focalizzarsi su come la sicurezza informatica supporterà e consentirà la crescita aziendale.
Qual è lo scopo di tutto ciò? Integrare la sicurezza nei processi aziendali fin dall'inizio e creare un ambiente di lavoro più sicuro per tutti. La sicurezza dovrebbe essere un principio chiave man mano che le tecnologie emergenti si spostano al centro della scena; per raggiungere questi obiettivi, le organizzazioni avranno bisogno di una strategia di sicurezza informatica innovativa piuttosto che rispondere in modo frammentario e reattivo.

Le quattro componenti vitali per rendere la sicurezza informatica parte della strategia di crescita sono (Antonucci, 2017):

1. supervisione strategica;
2. leadership;
3. digitalizzazione; poiché le organizzazioni fanno un uso maggiore delle tecnologie digitali, quanto aumenta la vulnerabilità della cyber sicurezza?
4. Tecnologie emergenti. Dove le organizzazioni stanno aumentando gli investimenti nella sicurezza informatica al fine di costruire questa secondo la progettazione?

Sulla base dell'indagine di quest'anno, purtroppo, solo un numero limitato di organizzazioni è preoccupato per le vulnerabilità causate dalle tecnologie emergenti. Questo è pericoloso considerando che le medesime tecnologie sono disponibili anche agli altri aggressori. Comunque, diverse organizzazioni ora considerano le tecnologie

emergenti come una spesa prioritaria per la sicurezza informatica, anche se persiste per troppe imprese una resistenza a proteggersi, dovuta alla spesa.

2.5.1. LA SUPERVISIONE STRATEGICA

L'impresa ha strutture che rendono la sicurezza informatica un elemento chiave della pianificazione strategica? Il 70% circa delle organizzazioni afferma che la propria leadership senior ha una comprensione globale della sicurezza o sta adottando misure positive per migliorare la propria comprensione, tuttavia, le organizzazioni più grandi hanno fatto più progressi: il 73% ha almeno una comprensione limitata rispetto al 68% delle controparti più piccole (van Kessel, 2019).
Bisogna assistere ad un rapido aumento della sicurezza in base alla progettazione, poiché molte organizzazioni stanno perseguendo la trasformazione digitale a un ritmo vertiginoso e sussiste il pericolo che la sicurezza informatica venga trascurata.

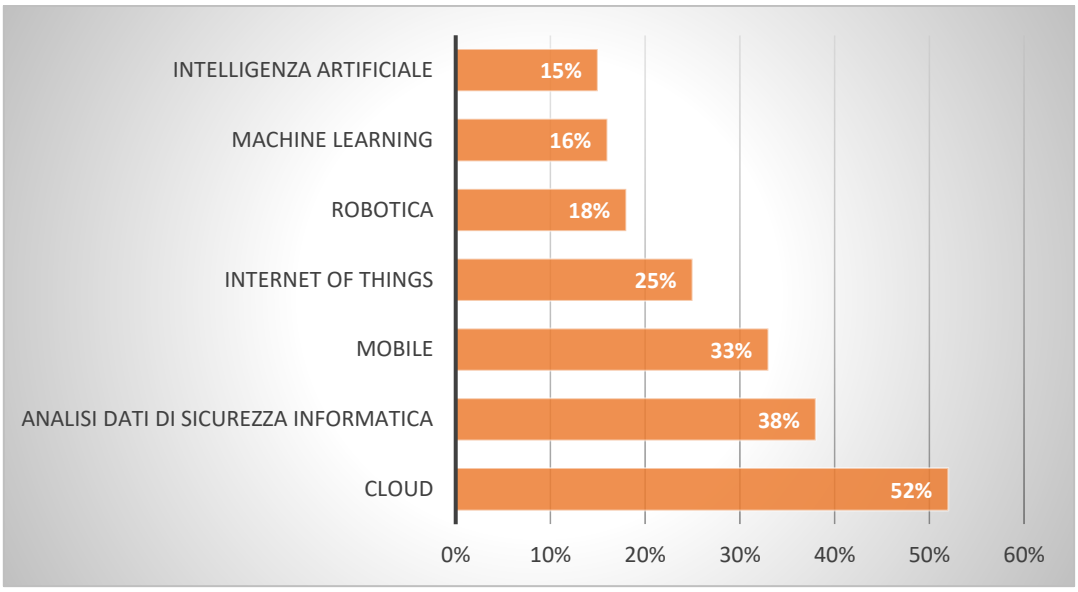
2.5.2. LEADERSHIP

Chi è responsabile in ultima analisi della sicurezza informatica? Per il 40% delle organizzazioni, il Chief Information Officer (CIO) si assume questa responsabilità, infatti quattro organizzazioni su 10 affermano che la persona investita della massima responsabilità è un membro del consiglio di amministrazione o della direzione.
Man mano che la sicurezza diventa un fattore chiave per la crescita, è probabile che questa percentuale aumenti; infatti, attualmente le organizzazioni più piccole hanno maggiori probabilità di avere responsabilità sulla sicurezza delle informazioni a livello di board, rispetto alle organizzazioni più grandi (Hasib, 2014).
Stanno emergendo anche nuovi tipi di ruoli. Stiamo assistendo alla nascita del Chief Security Officer (CSO) che potrebbe riferirsi a un responsabile delle informazioni e della sicurezza (CISO) o persino a un CIO, ma si trova al di fuori dell'organizzazione. Il CSO possiede responsabilità per il rischio cyber, il rischio per la sicurezza fisica e il rischio per la sicurezza personale, mentre il CISO o il CIO sono quelli focalizzati su una più ampia trasformazione informatica.

2.5.3. DIGITALIZZAZIONE

Mentre le organizzazioni perseguono la trasformazione, come aumenta il loro profilo di rischio, e quali minacce rappresentano le nuove tecnologie?

Figura 2.9: Rischi associati al crescente uso dei dispositivi mobili.

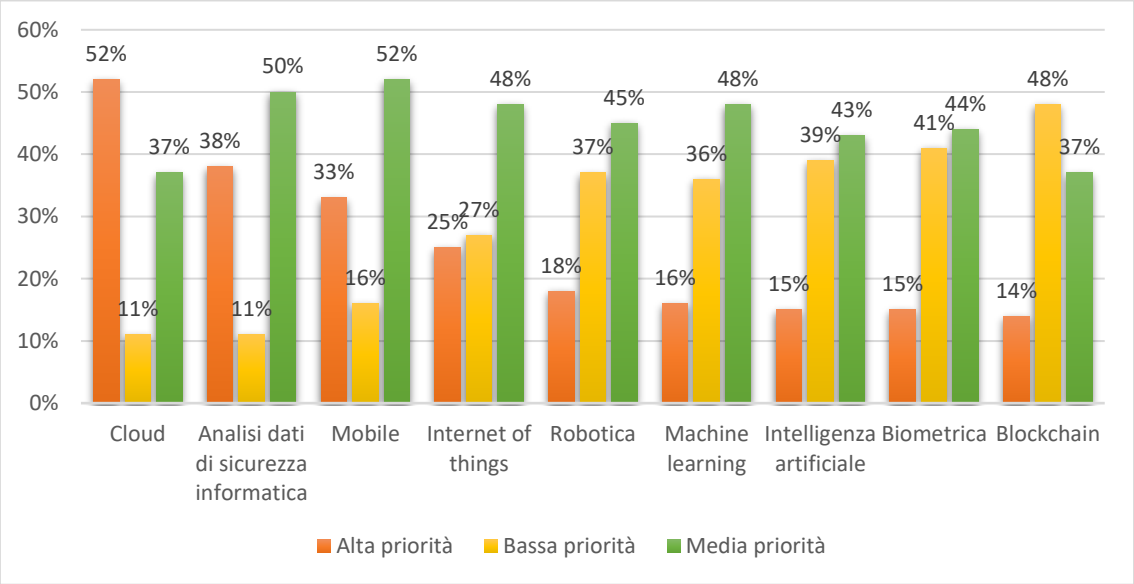


Fonte: The Cyber Risk Handbook (Antonucci, 2017).

2.5.4. TECNOLOGIE EMERGENTI

Dove assegnare la priorità agli investimenti dal punto di vista della sicurezza informatica e come promuovere la sicurezza in base alla progettazione?

Figura 2.13: Priorità degli investimenti sulla sicurezza informatica nel 2019.



Fonte: ISACA survey (Downs, 2019).

2.6. IL GDPR E LA SUA IMPLEMENTAZIONE

Navigando in rete è possibile notare che, ogni qualvolta si entra in un sito, compare un banner attestante che il sito in questione sta utilizzando i cookies e ci chiede se accettarli o meno. Questo è uno degli effetti del Regolamento UE 2016/679, noto come GDPR. GDPR è l'acronimo di General Data Protection Regulation ed è un regolamento scritto dall'Unione Europea, entrato in vigore il 25 maggio 2018 per modernizzare le leggi, che proteggono le informazioni personali e, a sostegno di ciò, l'NCSC[32] ha collaborato con l'ICO[33] per sviluppare una serie di risultati sulla sicurezza (Guide to the General Data Protection Regulation; ICO, 2018).

Tale regolamento stabilisce norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché norme relative alla libera circolazione di tali dati (Art.1 del Regolamento UE 2016/679).

"Il GDPR è una svolta per la protezione dei dati, ma è solo un'evoluzione, non una rivoluzione" (Denham, 2018).

[32] National Cyber Security Center.

[33] L'Information Commissioner's Office (ICO) è l'autorità di vigilanza del Regno Unito per il GDPR ed è responsabile della promozione e dell'applicazione della legislazione, oltre a fornire consulenza e orientamento a organizzazioni e individui.

Prima che tale regolamentazione iniziasse a essere applicata infatti, le precedenti norme sulla protezione dei dati in Europa erano state create negli anni '90 e avevano faticato a tenere il passo con i rapidi cambiamenti tecnologici.

Questo regolamento si applica a tutte le imprese che trattano di dati personali di cittadini dell'UE, ma anche le aziende fuori dall'Europa devono rispettarlo nel caso in cui trattino dati di cittadini europei[34].

Il principale obiettivo di questa nuova legislazione è quello di modificare il modo in cui le aziende e le organizzazioni del settore pubblico possano gestire le informazioni dei propri clienti, aumentare i diritti degli individui e dare loro un maggiore controllo sulle informazioni (Voigt, 2017)

Ma cosa significa GDPR a livello di sicurezza informatica? Il GDPR richiede che i dati personali vengano elaborati in modo sicuro, utilizzando adeguate misure tecniche e organizzative. Il regolamento non impone una serie specifica di misure di sicurezza informatica, ma si aspetta piuttosto che vengano intraprese azioni "appropriate"; in altre parole, è necessario gestire il rischio. Ciò che è appropriato dipenderà dalle circostanze, dai dati elaborati e quindi dai rischi posti, tuttavia, c'è un'aspettativa a proposito dell'adozione di misure di sicurezza minime e prestabilite. Esse devono essere progettate nei sistemi fin dall'inizio (denominate Privacy by Design) e mantenute efficaci per tutta la vita del sistema (Goddard, 2017).

[34] Secondo l'art.4 del Regolamento UE 2016/679:

1. Il presente regolamento si applica al trattamento dei dati personali effettuato nell'ambito delle attività di uno stabilimento da parte di un titolare del trattamento o di un responsabile del trattamento nell'Unione, indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione.

2. Il presente regolamento si applica al trattamento dei dati personali di interessati che si trovano nell'Unione, effettuato da un titolare del trattamento o da un responsabile del trattamento che non è stabilito nell'Unione, quando le attività di trattamento riguardano:

a) l'offerta di beni o la prestazione di servizi ai suddetti interessati nell'Unione, indipendentemente dall'obbligatorietà di un pagamento dell'interessato; oppure
b) il monitoraggio del loro comportamento nella misura in cui tale comportamento ha luogo all'interno dell'Unione.

3. Il presente regolamento si applica al trattamento dei dati personali effettuato da un titolare del trattamento che non è stabilito nell'Unione, ma in un luogo soggetto al diritto di uno Stato membro in virtù del diritto internazionale pubblico.

2.6.1. COME VENGONO DEFINITI I DATI PERSONALI

Il termine "dati personali" è il protagonista del regolamento generale sulla protezione dei dati (GDPR), infatti, solo se un trattamento di dati riguarda quelli personali, si applica il GDPR (Irwin, 2018).

Il termine è definito nell'Art.4 comma 1: I dati personali sono qualsiasi informazione correlata a una persona fisica identificata o identificabile. Poiché la definizione include "qualsiasi informazione", si deve presumere che il termine "dati personali" debba essere interpretato nel modo più ampio possibile, tuttavia, esistono diversi tipi di dati che permettono di identificare una persona (Art.9 del Regolamento UE 2016/679):

- i dati che permettono l'identificazione diretta della persona come un nome, cognome, un'immagine o un numero di identificazione, e i dati che consentono di riconoscere una persona, ma in maniera indiretta, come quelli di localizzazione, informazioni che esprimono il carattere fisico, fisiologico, genetico, identità mentale, commerciale, culturale o sociale. In pratica, questi includono anche tutti i dati che sono o possono essere assegnati a una persona in qualsiasi modo, ad esempio, il numero di telefono, carta di credito, i dati dell'account, la targa, l'aspetto, il numero cliente o l'indirizzo sono tutti dati personali.
- I dati personali sensibili sono un insieme specifico di "categorie speciali" che devono essere trattati con maggiore sicurezza. Ciò include le informazioni relative a:
    - i) origine razziale o etnica;
    - ii) opinioni politiche;
    - iii) credenze religiose o filosofiche;
    - iv) appartenenza sindacale;
    - v) dati genetici e dati biometrici utilizzati al fine di identificare in modo univoco qualcuno (Considerando 35, Regolamento UE 2016/679).
- Dati relativi a condanne penali e reati.

La Corte di giustizia europea considera anche informazioni meno esplicite, come le registrazioni degli orari di lavoro che includono informazioni sull'ora in cui un dipendente inizia e termina la sua giornata lavorativa, nonché su pause o orari che non rientrano nell'orario di lavoro, come dati personali (Irwin, 2018).

Inoltre, le risposte scritte di un candidato durante un test e qualsiasi commento

dell'esaminatore in merito a tali risposte sono "dati personali" se il candidato può essere identificato in maniera teorica. Lo stesso vale anche per gli indirizzi IP, se il responsabile del trattamento ha la possibilità legale di obbligare il fornitore a consegnare informazioni aggiuntive, che gli consentano di identificare l'utente per mezzo dell'indirizzo IP, si tratta anche in questo caso di dati personali.

Si deve notare per giunta che i dati personali non devono essere obbligatoriamente obiettivi, poiché informazioni soggettive come opinioni, giudizi o stime possono essere considerati dati personali, pertanto, ciò include una valutazione del merito creditizio di una persona o una stima delle prestazioni lavorative da parte di un datore di lavoro (Goddard, 2017).

Ultimo ma non meno importante, la legge afferma che le informazioni personali devono fare riferimento a una persona fisica, in altre parole, la protezione dei dati non si applica alle persone giuridiche come società, fondazioni e istituzioni. Per le persone fisiche, invece, inizia la protezione che si estingue con capacità giuridica[35].

2.6.2. *COME CONFORMARSI AL GDPR*

Il GDPR è ufficialmente entrato in vigore il 25 maggio 2018 e le aziende si sono dovute adattare a questa nuova normativa europea sulla privacy e sul controllo dei dati, poiché la mancata conformità può portare a sanzioni anche molto elevate (Voigt, 2017).

È essenziale comprendere le possibili implicazioni riguardo l'adeguatezza al GDPR e disporre di un piano, perché potrebbe essere necessario rivedere il proprio approccio alla governance e alla gestione dei dati.

Il GDPR concentra la sua attenzione sulla documentazione che i responsabili del trattamento dei dati devono conservare per dimostrare la loro responsabilità.

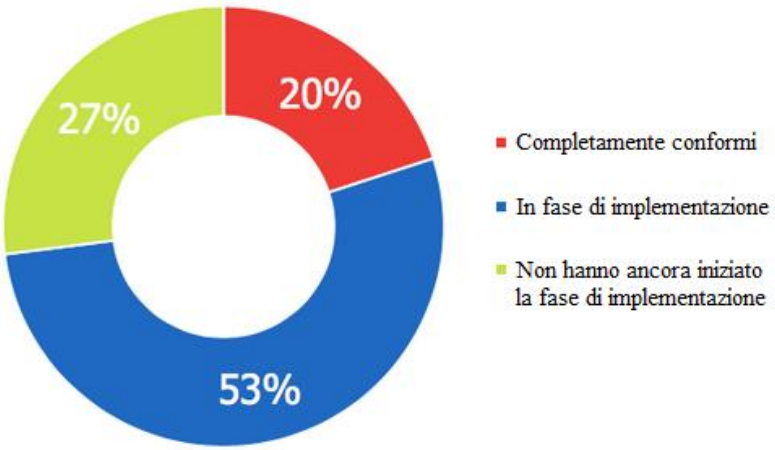
Coloro che già stavano rispettando il Data Protection Act (DPA[36]), disporranno di un approccio alla conformità valido ai sensi del GDPR, tuttavia, ci sono alcuni nuovi elementi e miglioramenti significativi, quindi alcune operazioni dovranno essere svolte in maniera diversa.

[35] Fondamentalmente, una persona fisica ottiene questa capacità con la sua nascita e la perde alla sua morte

[36] Il Data Protection Act 1998 era un atto del Parlamento del Regno Unito progettato al fine di proteggere i dati personali archiviati su computer o in un sistema di archiviazione cartacea organizzato. Ha emanato le disposizioni della Direttiva UE sulla protezione dei dati del 1995 in materia di protezione, trattamento e circolazione dei dati.

Più di 1 società su 4 (27%) deve ancora iniziare a lavorare per rendere la propria organizzazione conforme al GDPR, a più di 12 mesi di distanza dalla sua emissione (Babel, 2019).

Figura 2.10: Fase di conformità delle imprese rispetto al GDPR.



Fonte TrustArc report (Babel, 2019).

Le aziende dovrebbero seguire 12 passi in modo tale da assicurarsi di essere conformi al GDPR (Guide to the General Data Protection Regulation; ICO, 2018):

1. aumentare la propria consapevolezza riguardo al cambiamento delle leggi sulla protezione dei dati. Ciò potrebbe avere implicazioni significative in termini di risorse e, se lasciato all'ultimo minuto, potrebbe essere difficile prepararsi per un periodo di tempo limitato.
2. Documentare tutto (i dati personali in possesso, da dove provengono e con chi sono condivisi). Il GDPR richiede di conservare i registri delle attività, quindi sarà necessario organizzare un controllo delle informazioni all'interno dell'organizzazione o all'interno di particolari aree aziendali.
3. Rivedere le note sulla privacy. Ai sensi del Data Protection Act (DPA) vigente, le aziende forniscono informazioni come identità e scopo durante la raccolta dei dati personali. Questo di solito avviene attraverso un avviso sulla privacy, tuttavia, ai sensi del GDPR, ci sono alcuni dettagli aggiuntivi da condividere in un linguaggio conciso, facile da capire e chiaro, ad esempio, spiegare le basi legali dell'elaborazione dei dati, il periodo di

conservazione e il diritto delle persone di sporgere denuncia all'ICO in caso di problemi di gestione delle informazioni.

4. Controllare le procedure già in atto assicurandosi che coprano tutti i diritti delle persone. Il GDPR include i seguenti diritti per gli individui:

   i) il diritto di essere informati, ciò riguarda qualsiasi raccolta di dati da parte delle aziende e le persone devono essere informate precedentemente alla raccolta dei dati. I consumatori devono optare per la raccolta dei loro dati e il consenso deve essere fornito liberamente anziché implicito.

   ii) Il diritto di accesso. Le persone hanno il diritto di richiedere l'accesso ai propri dati personali e di chiedere come essi vengano utilizzati dalla società dopo che sono stati raccolti. La società deve fornire una copia dei dati personali, gratuitamente e in formato elettronico se richiesto.

   iii) Il diritto di correggere le informazioni garantisce che le persone possano aggiornare i propri dati se non aggiornati, incompleti o errati.

   iv) Il diritto all'oblio. Se i consumatori non sono più clienti o se ritirano il consenso da un'azienda per utilizzare i propri dati personali, hanno il diritto di cancellarli.

   v) Il diritto di limitare l'elaborazione. Gli individui possono richiedere che i loro dati non vengano utilizzati per l'elaborazione. Il loro record può rimanere al suo posto, ma non può essere utilizzato.

   vi) Il diritto alla portabilità dei dati. Gli individui hanno il diritto di trasferire i propri dati da un fornitore di servizi a un altro e questo deve accadere in un formato comunemente usato e leggibile dalla macchina.

   vii) Il diritto di opposizione che include il diritto delle persone di interrompere il trattamento dei propri dati per il marketing diretto. Non ci sono esenzioni a questa regola e qualsiasi elaborazione deve essere interrotta non appena la richiesta

viene ricevuta, inoltre, questo diritto deve essere chiarito alle persone all'inizio di ogni comunicazione.

viii) Il diritto alla notifica per cui se si è verificata una violazione che compromette i dati personali di una persona; quest'ultima ha il diritto di essere informata entro 72 ore dalla prima presa di coscienza della violazione.

Generalmente i diritti che gli individui posseggono ai sensi del GDPR sono gli stessi di quelli previsti dal DPA, ma con qualche miglioramento significativo. Il diritto alla portabilità dei dati, tuttavia, rappresenta una novità e si applica sia ai dati personali forniti da una persona a un responsabile del trattamento basato sul consenso dell'individuo o per l'esecuzione di un contratto, che al momento di esecuzione dell'elaborazione con mezzi automatizzati.

5. È necessario aggiornare le procedure e pianificare il modo di gestione delle richieste future.
6. Identificare, documentare ed esplicitare le basi legali. Ai sensi del GDPR, i diritti di alcune persone verranno modificati sulla base legale dell'utente per l'elaborazione dei dati personali.
7. Aggiornare i consensi esistenti. Se si utilizza il consenso come base per l'elaborazione e i consensi esistenti non soddisfano lo standard GDPR, è necessario rivedere il modo in cui si cerca, registra e gestisce il consenso in breve tempo.
8. Proteggere i dati dei bambini. Bisogna dotarsi di sistemi per verificare l'età o ottenere il consenso dei genitori/tutori perché il GDPR offre una protezione speciale per i dati personali dei minori.
9. È necessario predisporre procedure per rilevare, segnalare e indagare in modo efficace sulle violazioni dei dati personali. Il GDPR introdurrà l'obbligo per tutte le organizzazioni di segnalare determinati tipi di violazione dei dati all'ICO e, in alcuni casi, alle persone coinvolte. Fondamentale quindi notificare all'ICO una violazione laddove essa possa comportare un rischio per i diritti e le libertà delle persone.
10. Adottare un approccio alla privacy e alla protezione dei dati. Precedentemente visto come un advisory, il GDPR ha ora reso l'approccio

alla privacy e alla protezione dei dati un requisito legale esplicito. È fondamentale una valutazione dell'impatto sulla protezione dei dati (DPIA) in situazioni in cui l'elaborazione può comportare rischi elevati per le persone.

11. Designare un responsabile della protezione dei dati (DPO). È necessario designare un DPO se si è:
    - un'autorità pubblica (ad eccezione dei tribunali che agiscono nella loro capacità giudiziaria);
    - un'organizzazione che effettua il monitoraggio regolare e sistematico delle persone su larga scala; o
    - un'organizzazione che esegue l'elaborazione su larga scala di categorie speciali di dati, come cartelle cliniche o informazioni su condanne penali.
12. Determinare l'autorità principale. Ciò è rilevante solo quando si commercia a livello internazionale, ma, se questo si applica alla propria impresa, è necessario mappare dove l'organizzazione prenda le decisioni più significative sulle sue attività di elaborazione.

I dati rappresentano un nuovo tipo di valuta in questo mondo evoluto e il GDPR non ha solo impatti negativi per le aziende, ma crea anche opportunità.
Le imprese che dimostrano di apprezzare la privacy di un individuo (al di là della semplice conformità legale), che sono trasparenti su come vengono utilizzati i dati, che progettano e implementano modi nuovi e migliorati da gestione dei dati dei clienti durante tutto il loro ciclo di vita, costruiscono una fiducia più profonda e mantengono clienti più fedeli (Irwin, 2018).

2.6.3 SANZIONI

Le autorità nazionali possono o devono valutare multe per violazioni specifiche della protezione dei dati conformemente al regolamento generale sulla protezione di questi (GDPR-info.eu).
Le multe vengono applicate in aggiunta o al posto di ulteriori rimedi o ordini correttivi, come l'ordine di porre fine a una violazione, un'istruzione per adeguare il trattamento dei

dati al rispetto del GDPR, nonché il potere di imporre una limitazione temporanea o definitiva, compreso un divieto al trattamento dei dati. Le ammende devono essere efficaci, proporzionate e dissuasive per ogni singolo caso in cui decidere se e quale livello di sanzione può essere valutato, le autorità dispongono di un catalogo statutario di criteri; tra l'altro, l'infrazione intenzionale, la mancata adozione di misure per mitigare il danno verificatosi o la mancanza di collaborazione con le autorità possono aggravare la situazione con conseguenza di incremento della sanzione.

Per violazioni particolarmente gravi, elencate nell'Art. 83 comma 5 del GDPR, l'ammenda può arrivare fino a 20 milioni di euro o, nel caso di una grande impresa, fino al 4% del fatturato globale totale dell'anno fiscale precedente, se superiore.

Secondo il catalogo di violazioni meno gravi previste nell'art. 83 comma 4 invece, la sanzione sarà dimezzata fino a 10 milioni di euro o, nel caso di una grande impresa, fino al 2% dell'intero fatturato globale dell'anno fiscale precedente, a seconda di quale sia maggiore.

Particolarmente importante qui, il termine "impresa", equivalente a quello usato nell'Art. 101 e 102 del trattato sul funzionamento dell'Unione europea (TFUE), dove essa comprende ogni entità impegnata in un'attività economica, indipendentemente dallo status giuridico dell'entità o dal modo in cui essa è finanziata.

Un'impresa non può quindi consistere solo in una singola azienda nel senso di persona giuridica, ma anche in diverse persone fisiche o giuridiche, pertanto, un intero gruppo può essere trattato come un'unica impresa e il suo fatturato annuo globale in tutto il mondo può essere utilizzato per calcolare l'ammenda causata da una violazione del GDPR da parte di una delle sue società. Inoltre, ciascuno Stato membro stabilisce norme sulle altre sanzioni per le violazioni del regolamento, che non siano già coperte dall'art. 83. Molto probabilmente queste sono penali per determinate violazioni del GDPR o riguardanti violazioni delle norme nazionali adottate sulla base delle clausole di flessibilità del GDPR (Guide to the General Data Protection Regulation; ICO, 2018).

Le sanzioni nazionali devono anche essere efficaci, proporzionate e fungere da deterrente. Una situazione punibile in una società può essere smascherata attraverso un’attività di ispezione proattiva, condotte dalle autorità per la protezione dei dati, da un dipendente insoddisfatto, da clienti o potenziali clienti che si lamentano con le autorità.

Un esempio del fatto che le conformità e relative sanzioni non debbano essere prese alla leggera ce lo offre il colosso Google, che ha ricevuto una multa di oltre 50 milioni di euro per la violazione del GDPR in Francia. Il regolatore francese per la protezione dei dati,

CNIL, ha emesso a Google tale ammenda nel gennaio del 2019 poiché non è riuscita a fornire informazioni sufficienti agli utenti in merito alle proprie politiche di consenso dei dati non offrendo loro un controllo sufficiente sull'utilizzo delle loro informazioni (Selby, 2019).

Questa è la più eclatante multa mai emessa ai sensi del GDPR ed è la prima volta che uno dei giganti della tecnologia ha infranto le dure nuove normative entrate in vigore.

Capitolo 3

3. CYBER INSURANCE: DEFINIZIONE, RUOLO E INTERAZIONI

3.1. CHE COS'E' LA CYBER INSURANCE?

Gestire i problemi di privacy e protezione dei dati di oggi non è un'impresa facile. Iperconnessione[37], analisi di big data e accesso remoto ai dati aziendali hanno rivoluzionato il modo in cui funzionano le imprese moderne, ma questi stessi fenomeni hanno anche ampliato in modo esponenziale l'esposizione di privacy e protezione dei dati che le aziende devono ora gestire (Evans, 2019).

Il rischio è enorme in qualsiasi fase del ciclo di vita delle informazioni: dalla creazione o raccolta di informazioni, il loro utilizzo, la conservazione, e collocazione finale (Antonucci, 2017).

La violazione e l'abuso dei dati, la criminalità informatica e un panorama normativo in evoluzione e sempre più rigoroso sono ora riconosciuti come preoccupazioni a livello aziendale, ma, nonostante i notevoli sforzi e l'aumento della spesa, anche le imprese più scrupolose non devono commettere l'errore di sentirsi intoccabili (Bechelli, 2019). Indipendentemente dalle dimensioni dell'azienda o dal settore, sono inevitabili incidenti riguardanti la privacy e protezione dei dati, per questo motivo, sempre più aziende domandano la cyber insurance, come copertura contro questi implacabili rischi (Burns et al., 2018).

All'inizio del nuovo millennio gli assicuratori hanno iniziato a offrire polizze orientate alla protezione da: perdite finanziarie a causa di violazioni dei dati, interruzione dell'attività, sottrazione di dati, estorsione, costi di gestione delle crisi e responsabilità derivanti dalle violazioni. Dopo che, le più importanti nazioni hanno iniziato a emanare leggi sulla notifica delle violazioni dei dati, a partire dal 2003, è cresciuta la necessità di una copertura assicurativa progettata in modo da affrontare i costi relativi a questi nuovi

[37] Questo termine possiamo definirlo come "il bisogno di rimanere collegati a internet e ai social network", la cui necessità risulta più forte rispetto al fumare una sigaretta, bere una bevanda alcolica o avere rapporti sessuali (Arnold et al., 2012).

obblighi e passività associate. Decine di assicuratori offrono un certo tipo di copertura contro i rischi informatici, mentre i sottoscrittori si sforzano di affrontare nuove e urgenti minacce informatiche, che sono in continua evoluzione.

A livello base, la cyber insurance fornisce il necessario supporto finanziario per le aziende che si trovano ad affrontare un incidente informatico: la copertura di prima parte della polizza si applica ai costi sostenuti dall'assicurato quando esso risponde direttamente a un evento informatico, mentre la copertura di terzi fornisce una protezione da responsabilità nel caso in cui la compagnia assicurata commetta un errore, che comporti una violazione di dati o attacco informatico ai danni di un cliente (Selby, 2019).

A differenza di molte altre linee assicurative più tradizionali, non esiste un modulo standard per l'assicurazione informatica. Più di 150 assicuratori attualmente vendono la copertura informatica e ognuno ha la propria forma di polizza, utilizzando un proprio linguaggio; diventa quindi una sfida per le aziende cercare di confrontare una polizza assicurativa informatica con un'altra[38]. Tuttavia, dal momento che il mercato delle cyber assicurazioni è piuttosto competitivo, gli assicurati hanno spesso la possibilità di cercare e negoziare condizioni di copertura più favorevoli.

3.1.1. COPERTURA DI PRIMA PARTE

Le first party coverage (coperture di prima parte) sono le più utilizzate e comprendono servizi legali e forensi per determinare se si sia verificata o meno una violazione e, in caso affermativo, aiutare con: la conforme normativa, i costi per informare i dipendenti interessati e/o terze parti e costi di notifica della data violazione (Kazan, 2017).

La copertura è di solito disponibile anche per i costi di interruzione della rete e delle attività commerciali, danni ai dati digitali, recupero della reputazione dell'assicurato e pagamento delle eventuali richieste di riscatto.

In caso di violazione dei dati, l'assicurazione informatica in genere prevede assistenza legale[39] al fine di coordinare la risposta dell'assicurato all'incidente informatico (Selby, 2019).

[38] Ad esempio, due moduli possono utilizzare gli stessi termini, come "evento di sicurezza" o "indagine normativa", ma definiranno tali termini in modo diverso, creando differenze significative nella portata della copertura fornita.

[39] Un coach esperto può costituire un efficace team di specialisti e guidare in modo efficiente l'azienda attraverso le questioni legali, normative e le pubbliche relazioni derivanti da un incidente riguardante la sicurezza informatica.

Date le complessità delle varie leggi relative alla notifica della violazione dei dati, alle crescenti richieste dei regolatori, al controllo dei media e ad azioni collettive, il mantenimento di un coach qualificato è forse il più grande vantaggio inserito in questo tipo di assicurazione.
Esempi di scenari di coperture di prima parte sono:

- Costi legali e informatici a seguito di una violazione dei dati;
- costi di gestione delle crisi;
- ripristino dei dati dell'assicurato;
- costi derivanti da un attacco DDoS (Distributed Denial of Service);
- perdita di entrate aziendali e spese aggiuntive a seguito di un'interruzione dell'attività;
- pagamento della domanda di estorsione informatica;
- perdita derivante dal trasferimento di fondi in base a istruzioni provenienti da e-mail fraudolente.

3.1.2. COPERTURA DI TERZE PARTI

La copertura di terze parti può essere racchiusa in vari modi, tra cui rivendicazioni per violazione della privacy, uso improprio dei dati personali, diffamazione/calunnia o trasmissione di contenuti dannosi (Kshetri, 2018).
La copertura è disponibile per i costi legali, di risarcimenti o danni, che l'assicurato deve pagare a seguito di: una violazione, responsabilità dei media elettronici[40], multe e sanzioni. Esempi di scenari e costi di copertura di terze parti sono (Selby, 2018):

- class action legali del consumatore a seguito di una violazione dei dati;
- cause legali dell'emittente della carta di credito a seguito di clonazione dei dati della carta;
- indagine normativa a seguito di violazioni;
- cause legali relative a diffamazione o calunnia rispetto al contenuto del sito Web dell'assicurato;
- reclami basati sulla trasmissione di virus da parte di assicurati a terzi;

[40] La elettronic media liability comprende la violazione di copyright, nome di dominio o nomi commerciali su un sito internet.

- reclami nei confronti di direttori e funzionari per inadeguata sorveglianza della sicurezza informatica.

3.1.3. COPERTURA DELLE RICHIESTE DI RISARCIMENTO

Diversamente dalle polizze assicurative commerciali tradizionali, che sono disponibili su una struttura di copertura sinistri o basata sulla ricorrenza, la copertura informatica è attualmente disponibile solo su base sinistri (Selby, 2020).
In base a una polizza di sinistro, il fattore scatenante della copertura è una richiesta di risarcimento presentata dal contraente durante il periodo di polizza. Gli assicurati spesso sono in grado di ottenere un "periodo di rendicontazione esteso", che può sostanzialmente prolungare il periodo di tempo, durante il quale una richiesta di risarcimento deve essere presentata all'assicuratore.

3.1.4. COPERTURA RETROATTIVA

Dal momento che gli incidenti informatici possono non essere rilevati per mesi o addirittura anni, le aziende dovrebbero considerare di possedere violazioni di dati non rilevate al momento della domanda e tentare di garantire la copertura, che potrebbe applicarsi a tutti gli eventi non rilevati. L'offerta di una copertura retroattiva dipende in larga misura dall'assicuratore e dal profilo di rischio unico del potenziale assicurato (Gold, 2017)

3.1.5. GARANZIE ACCESSORIE

Fortunatamente, le recenti iterazioni di polizze informatiche vanno ben oltre la copertura della violazione dei dati, e offrono protezione contro una vasta gamma delle più fastidiose minacce informatiche, che colpiscono le aziende in ogni settore commerciale (Selby, 2019).
Alcune delle principali esposizioni per le quali potrebbe essere disponibile la copertura sono:

- estorsione; la copertura è generalmente disponibile per i pagamenti di

ransomware, nonché per altri tipi di cyber estorsioni, come le minacce di divulgare pubblicamente informazioni protette o di interrompere i sistemi informatici dove alcuni assicuratori aiuteranno nel pagamento del riscatto tramite valuta digitale;

- ingegneria sociale; alcuni assicuratori offrono una copertura in base al tipo di polizza che si applica espressamente a phishing o ad altri attacchi, che inducono un assicurato a trasferire i fondi dell'azienda a terzi[41];
- copertura delle perdite per dirigenti. Alcune compagnie di assicurazione forniscono copertura per il furto di identità e il furto di fondi da conti bancari personali di funzionari esecutivi, derivanti da una violazione di terze parti della sicurezza di rete della società;
- furto di identità aziendale; la copertura può essere disponibile per le perdite subite a seguito di un uso fraudolento dell'identità elettronica della società, inclusa la creazione di credito a nome della società, la firma elettronica del contratto e la creazione di un sito web progettato per impersonare la società;
- eventuale interruzione dell'attività; è possibile che qualche società di assicurazioni offra copertura per la perdita di guadagno, spese legali e spese extra sostenute a seguito dell'interruzione delle attività commerciali dell'assicurato causata da un blackout involontario e non pianificato di sistemi informatici gestiti da un'azienda terza, che fornisce prodotti o servizi necessari all'assicurato ai sensi di un contratto scritto[42];
- violazione del telefono; le aziende potrebbero essere in grado di ottenere una copertura per le perdite derivanti dall'hacking del proprio sistema telefonico, incluso il rimborso dei costi per le chiamate non autorizzate;
- responsabilità della direzione; la copertura può essere disponibile per alti dirigenti, se essi vengono citati in giudizio in relazione a un evento informatico coperto;
- perdita reputazionale; questa copertura indennizza l'assicurato per il mancato guadagno durante un periodo di tempo definito (ad es. 30 giorni) a seguito di un evento di violazione di informazioni;
- danni materiali e lesioni personali; copertura se un attacco informatico provoca

[41] Ciò si verifica spesso quando un dipendente della compagnia assicurata riceve un'e-mail fraudolenta contenente istruzioni finalizzate all'invio di un pagamento ad un qualche venditore estero.

[42] Questa copertura può essere particolarmente utile per le aziende che operano nell'economia digitale e interconnessa di oggi.

danni alla proprietà dell'assicurato o terzi oppure lesioni ai clienti dell'assicurato.

È importante notare, tuttavia, che le coperture sopra descritte potrebbero non essere disponibili da tutti gli assicuratori e non tutti gli assicurati si qualificherebbero per tutti i tipi di copertura; inoltre, alcune garanzie accessorie possono essere soggette a sotto-limiti e condizioni importanti, come la richiesta del consenso della compagnia assicurativa prima di incorrere in eventuali spese.
Anche se un vettore non offre in modo proattivo nessuna di queste coperture emergenti, può includere tale copertura, se richiesto da un assicurato, in particolare se l'assicuratore è a conoscenza del fatto che tale copertura venga offerta dai concorrenti (Gold, 2017).

3.2. OTTENERE LA GIUSTA COPERTURA ASSICURATIVA

Al fine di ottenere una copertura adeguata alle esigenze dell'azienda, è necessario seguire cinque passaggi (Selby, 2018).
Passaggio 1: identifica i tuoi pericoli informatici. Il primo passo nel processo dovrebbe essere una valutazione dell'esposizione di un'entità ai pericoli informatici. Non tutte le società sono uguali e ad esempio, i rischi di cyber e privacy per un rivenditore online sarebbero diversi da quelli di una società di consulenza. Non è consigliabile un approccio unico per questo passaggio, le aziende dovrebbero adottare un approccio a livello aziendale per garantire, che i rischi sostenuti da tutte le divisioni debbano essere affrontati all'interno dell'azienda e inclusi nella valutazione. Dovrebbero essere consultate più parti interessate all'interno dell'organizzazione e potenzialmente alcune parti esterne (fornitori di tecnologia, ad esempio) tra cui:

- operazioni di business;
- legale;
- gestione dei rischi;
- risorse umane;
- privacy e/o compliance;
- informatica e/o sicurezza delle informazioni;
- finanza.

Passaggio 2: esaminare il programma assicurativo esistente. Successivamente, le aziende

dovrebbero analizzare attentamente le loro polizze assicurative esistenti, per determinare come le coperture attuali si abbinino ai rischi informatici identificati.
Le polizze tradizionali in materia di proprietà e responsabilità, nonché sulla criminalità, possono contenere una certa protezione contro i rischi informatici.
Le polizze di rapimento e riscatto possono anche fornire una copertura per i rischi informatici associati a una domanda di estorsione; detto questo, molti assicuratori hanno preso provvedimenti per escludere i rischi legati alla cibernetica.
Le polizze contengono inoltre regolarmente esclusioni rivolte in particolare alla privacy e ai rischi informatici, come quelle per le richieste di risarcimento del TCPA (Telephone Consumer Protection Act).
La revisione del programma assicurativo è complicata dal fatto che la maggior parte delle entità è assicurata nell'ambito di una varietà di polizze assicurative, le quali devono essere considerate sia individualmente, che in relazione l'una con l'altra. A causa della complessità di questi problemi, le imprese dovrebbero prendere in considerazione la possibilità di rivolgersi a un consulente assicurativo esperto, che fornisca un'assistenza con questa analisi.

3.2.1. COPERTURA NELL'AMBITO DELLE POLIZZE TRADIZIONALI

Mentre la copertura assicurativa commerciale tradizionale può fornire alcune strade per mitigare il rischio in una violazione dei dati, le aziende potrebbero incorrere in un rischio, se si affidassero a tali polizze per la copertura primaria di violazioni dei dati.
Sebbene alcune aziende abbiano presentato con successo dichiarazioni sulle polizze tradizionali, affidarsi alle polizze tradizionali, per la copertura di un evento di violazione dei dati, è diventato sempre più incerto e molti assicuratori stanno combattendo vigorosamente le richieste di risarcimento informatico nell'ambito di polizze non informatiche (Selby, 2019).
Le polizze generali di responsabilità commerciale comprendono tre tipi di coperture:

A. copertura A, che copre lesioni personali e danni materiali;
B. copertura B, che copre lesioni personali e pubblicitarie;
C. copertura C, che copre i pagamenti medici per lesioni personali.

Queste polizze in genere definiscono un danno alla proprietà, come una lesione fisica o la perdita dell'uso di proprietà materiali e molte polizze specificano che i dati elettronici

non sono proprietà materiali; inoltre, la maggior parte delle polizze esclude anche danni alla proprietà dell'assicurato, oltre a ciò alcune aziende hanno presentato con successo richieste di risarcimento per violazione dei dati nell'ambito delle loro polizze tradizionali, in particolare con la copertura B, dove alcuni assicurati hanno richiesto con successo determinati tipi di esposizione, nell'ambito dell'assicurazione sulla responsabilità civile (EPL).

La maggior parte degli assicuratori ha tuttavia aggiunto nuove specializzazioni, che escludono specificamente la responsabilità derivante dalla divulgazione di informazioni riservate o personali.

3.2.2. CYBER ESCLUSIONE

L'ufficio dei servizi assicurativi (ISO) pubblica periodicamente le forme di polizze standard, che gli assicuratori utilizzano ampiamente; laddove non utilizzati nella loro interezza, gli assicuratori spesso adottano i moduli con una sostanziale standardizzazione (Burns, 2016).

Quando gli assicuratori hanno iniziato a includere esclusioni nelle loro tradizionali polizze commerciali, ISO ha approvato nuovi moduli per le specializzazioni facoltative, che escludono la copertura per richieste di risarcimento personali e pubblicitarie, derivanti dall'accesso o dalla divulgazione di informazioni riservate.

In particolare:

- CG 21 08 05 14 (esclusione: accesso o divulgazione di dati riservati o informazioni personali (solo copertura B)). Esclude la copertura per lesioni personali e pubblicitarie derivanti da qualsiasi accesso o divulgazione di informazioni riservate o personali anche se l'assicurato richiede danni per:
    - i) costi di notifica;
    - ii) spese di monitoraggio del credito;
    - iii) spese di indagine forense;
    - iv) spese di pubbliche relazioni; e
    - v) qualsiasi altra perdita, costo o spesa sostenuta a causa di accesso non autorizzato o divulgazione di informazioni personali.
- CG 21 07 05 14 (esclusione: accesso o divulgazione di dati riservati o informazioni

personali e responsabilità relativa ai dati: eccezione alle lesioni personali limitate non inclusa). È simile a CG 21 08 05 14 ma esclude anche la copertura per lesioni personali e danni alla proprietà derivanti da qualsiasi accesso o divulgazione di informazioni riservate o personali o dalla perdita o dal danneggiamento di dati elettronici.

- CG 21 06 05 14 (esclusione: accesso o divulgazione di informazioni riservate o informazioni personali e responsabilità relativa ai dati: con eccezione di lesioni personali). Simile a CG 21 07 05 14, ad eccezione del fatto che non sono esclusi i danni fisici derivanti dalla perdita o dal danneggiamento dei dati elettronici.

Gli assicuratori hanno ampiamente adottato questi moduli da quando ISO li ha resi disponibili nel 2014.

È importante sottolineare che, anche se una copertura è disponibile nell'ambito delle polizze tradizionali nonostante queste esclusioni o altre disposizioni di polizza, tale copertura probabilmente non sarà abbastanza ampia da includere sia la responsabilità, che i costi associati ad eventi informatici. Di conseguenza, sempre più aziende stanno cercando un'assicurazione informatica per una protezione più completa dagli eventi informatici.

Passaggio 3: richiesta di copertura informatica. Anche se non esiste un'applicazione standard per la cyber insurance, gli assicuratori di solito chiedono spesso la stessa tipologia di informazioni al potenziale assicurato, inclusi i consueti dati finanziari sulla società come attività e ricavi, numero di dipendenti e attività di fusione e acquisizione pianificate. Altre informazioni che possono richiedere al fine di stipulare questa particolare forma di polizza assicurativa sono (Selby, 2019) :

- volume e tipi di dati (ad es. dati delle carte di credito, registri bancari, informazioni sanitarie protette) conservati e gestiti dalla società;
- esistenza di polizze e procedure scritte relative al trattamento delle informazioni, approvate e aggiornate;
- conformità con gli standard e normative di sicurezza e frequenza delle valutazioni;
- programmi di sicurezza di rete esistenti, compreso l'uso di firewall, software antivirus e test di intrusione di rete;
- assunzione di un responsabile delle informazioni o della tecnologia;
- cronologia di incidenti e violazioni della sicurezza, incluso il tempo impiegato per rilevare eventuali violazioni precedenti;

- minacce precedenti che hanno disabilitato la rete o il sito web dell'azienda;
- consapevolezza di fatti o circostanze, che potrebbero ragionevolmente dar luogo a una richiesta di risarcimento ai sensi di una potenziale polizza informatica;
- cancellazione anticipata o rifiuto di rinnovare una determinata polizza informatica;
- budget per la sicurezza (fa parte del budget IT e in caso affermativo, in quale percentuale?);
- pratiche relative alla crittografia dei dati, password, patch e controllo dell'accesso al sistema;
- pratiche di assunzione e formazione dei dipendenti e procedure relative alla risoluzione;
- controlli di sicurezza fisica (ad es. carte d'accesso);
- audit di fornitori di servizi di terze parti;
- contratti e polizze del fornitore;
- polizze che regolano i dispositivi mobili e i social media;
- procedure di backup dei dati.

Bisogna porre attenzione a completare accuratamente la domanda, che diventerà parte della polizza emessa. Le applicazioni possono richiedere la firma del presidente, del CEO e/o del CIO della società, che deve attestare l'accuratezza delle risposte. Informazioni imprecise possono compromettere la copertura, se viene successivamente presentata una richiesta di risarcimento nell'ambito della polizza.

Passaggio 4: trovare la giusta copertura nel mercato dinamico delle cyber assicurazioni di oggi. La selezione di un'adeguata polizza assicurativa informatica può essere impegnativa; a differenza di quelle più tradizionali, non esiste un modulo standard di polizza assicurativa informatica e non tutte sono uguali. Ci possono essere differenze sostanziali in termini, definizioni ed esclusioni da una polizza all'altra, che possono avere un impatto significativo sulla copertura fornita. Ad esempio, due polizze possono fornire una copertura per un "evento di sicurezza informatica", ma una polizza che definisce in modo restrittivo il termine "evento di sicurezza informatica" può fornire una copertura sostanzialmente inferiore, rispetto ad un’altra con una definizione ampia o un termine funzionalmente equivalente.

Le decisioni prese rigorosamente sul prezzo possono rivelarsi in futuro più costose, infatti gli assicurati dovrebbero analizzare attentamente i moduli, per capire esattamente quale

tipo di copertura viene offerta.

I potenziali assicurati dovrebbero inoltre accertarsi che, qualsiasi polizza in esame si applichi al territorio di copertura appropriato (in tutto il mondo rispetto a un territorio più limitato) e che il fattore scatenante della copertura, attivata quando si verifica la perdita rispetto al momento in cui viene presentata la richiesta di risarcimento, sia adatto alle esigenze dell'azienda.

La copertura retroattiva è auspicabile per molte aziende, in particolare per i neo-cyber assicurati. Le esclusioni devono essere attentamente esaminate, nonché i limiti di polizza disponibili, i sub limiti, le franchigie e i premi.

Anche gli attributi della compagnia assicurativa possono essere rilevanti; gli assicurati potrebbero voler considerare la reputazione dell'assicuratore per la gestione dei sinistri, le sue capacità in caso di violazione, il periodo di tempo in cui ha fornito la copertura assicurativa informatica e il suo rating finanziario.

Ci possono anche essere differenze significative tra gli assicuratori in relazione alla fornitura di servizi gratuiti e/o scontati di controllo delle perdite informatiche, che possono essere abbastanza vantaggiosi: questi servizi possono includere strumenti di governance delle informazioni, consulenza sulla gestione delle informazioni, formazione dei dipendenti, valutazione dei rischi e revisione dei contratti con i fornitori.

Gli assicurati dovrebbero inoltre informarsi sulle pratiche dell'assicuratore relative all'utilizzo di fornitori di servizi di terze parti, ad esempio avvocati e consulenti, che assistono in caso di incidente informatico e coloro che si sentono tranquilli a lavorare con i propri fornitori, sono invitati a sollevare il problema durante il processo di negoziazione delle polizze.

Quando si seleziona una copertura informatica, gli assicurati possono spesso scegliere da un menù di diverse coperture che si applicano a una varietà di esposizioni, quali responsabilità di terzi, risposta alla violazione, estorsione, frode informatica, difesa normativa, responsabilità dei media del sito Web e interruzione dell'attività.

Una società che ha una buona conoscenza delle sue esposizioni al rischio informatico, sarà in grado di selezionare in maniera più vantaggiosa. Va notato, tuttavia, che alcuni tipi di copertura potrebbero non essere disponibili per tutti gli assicurati, a seconda di fattori come il raggruppamento del settore del singolo assicurato e il suo profilo di rischio: ad esempio, gli assicuratori probabilmente vorranno garantire che una società abbia piani e procedure di gestione delle crisi e di disaster recovery prima di emettere una copertura per interruzione dell'attività. Nel valutare le varie opzioni di copertura, i potenziali

assicurati devono fare affidamento sugli input ricevuti in merito al profilo di rischio cibernetico dell'azienda per garantire che, qualsiasi polizza informatica in esame risponda pienamente alle esigenze di copertura note.

Le molte differenze tra le varie coperture disponibili sul mercato rendono il confronto piuttosto impegnativo per i potenziali assicurati e la questione è ulteriormente complicata dal fatto che, gli assicuratori aggiornano e modificano frequentemente le proprie forme di polizza, a volte in modo abbastanza significativo, alla luce delle minacce emergenti e degli sviluppi del mercato. Con ciò, molto spesso, gli assicurati cercano consulenti esperti per farsi aiutare nel selezionare una copertura adeguata a soddisfare delle specifiche esigenze informatiche. Un consulente può fornire assistenza nella negoziazione di migliori termini di copertura, eliminazione di determinate esclusioni, revisione di condizioni, requisiti di polizza onerosi e consenso all'utilizzo dei fornitori di servizi preferiti dell'assicurato in caso di incidente informatico.

Un consulente può anche aiutare l'assicurato a garantire che, la sua copertura si combini in modo appropriato con le altre polizze assicurative nel suo portafoglio, al fine di evitare lacune, duplicità e altre questioni che possono portare a controversie con gli assicuratori o compromettere la copertura.

Un consulente può anche aiutare l'assicurato a comprendere le varie condizioni e requisiti contenuti nella polizza, in modo che l'assicurato possa adempiere alle proprie responsabilità ed evitare passi falsi che, potrebbero mettere a repentaglio la copertura in caso di sinistro.

3.2.3. PRINCIPALI PUNTI DI NEGOZIAZIONE

Quando si negozia l'acquisto di una polizza informatica, è necessario considerare, tra l'altro, i seguenti punti:

1. la polizza affronta ogni cyber risk dell’impresa?
2. I limiti e i sub limiti della polizza sono adeguati alle esigenze?
3. Esiste una copertura retroattiva per precedenti violazioni sconosciute?
4. Esiste una copertura per i reclami risultanti da errori dei fornitori?
5. È coperta la perdita di dati o solo il "furto" di essi?
6. La polizza copre i dati in possesso di fornitori di cloud e altre terze parti?
7. L'assicuratore offre una deroga alla surrogazione?

8. In che modo la cyber policy rientra nel programma assicurativo complessivo della compagnia?
9. È possibile negoziare disposizioni, limiti e premi più favorevoli con un altro assicuratore?
10. È possibile eliminare alcune esclusioni e, in caso negativo, limitarne la portata?

3.2.4. IMPORTANTI ESCLUSIONI DALLA POLIZZA

Come per tutte le polizze assicurative, gli assicurati devono esaminare attentamente le esclusioni e altre disposizioni di polizza che possono limitare la copertura. A causa della mancanza di moduli standardizzati, questo impegno è particolarmente importante nella scelta della copertura informatica. Attualmente, con varie limitazioni ed eccezioni, le polizze informatiche generalmente contengono esclusioni per reclami o perdite derivanti da:

- lesioni personali;
- danni materiali;
- responsabilità contrattuale;
- pratiche di lavoro;
- inquinamento;
- violazioni dell'antitrust;
- violazioni della legge sul reddito da lavoro (ERISA);
- violazioni del TCPA (Telephone Consumer Protection Act);
- raccolta, acquisizione o conservazione illecite di informazioni di identificazione personale (PII);
- atti, errori, incidenti o eventi che sono stati commessi o si sono verificati prima della data retroattiva della polizza.

Come notato, le eccezioni e le limitazioni si applicano spesso alle esclusioni delle polizze e alcuni assicuratori sono propensi a negoziare ulteriori limitazioni e persino a rimuovere alcune esclusioni; inoltre, alcuni assicuratori offrono copertura per alcune perdite tipicamente escluse, inclusi danni alla proprietà e lesioni personali, derivanti da un evento informatico coperto.
Alcuni assicuratori forniranno anche una copertura limitata per i reclami TCPA ed è

importante ricordare che, altri contratti possono avere un effetto esclusivo su un reclamo: ad esempio, supponiamo che una polizza fornisca copertura per le indagini normative solo se esse derivano da un "evento informatico[43]"; l'assicurato, pertanto, non avrebbe alcuna copertura per le indagini regolamentari, derivanti dalle sue pratiche illecite di raccolta e conservazione dei dati.

Come illustrato, le aziende devono rivedere attentamente tutti i termini definiti per valutare i loro effetti sulla copertura tali da garantire che non stiano selezionando involontariamente una polizza che escluda la copertura desiderata.

Passaggio 5: considerazioni post-copertura. Una volta stabilita la copertura, è fondamentale che, l'assicurato comprenda i vari requisiti e le condizioni di polizza a cui deve conformarsi. Questo dovrebbe anche prendere provvedimenti per comprendere i processi di sinistro, previsti dai termini della polizza in caso di incidente informatico coperto, monitorare e valutare periodicamente la propria copertura alla luce delle esigenze aziendali in evoluzione, comprese eventuali attività di fusione e acquisizione e il mercato della cyber insurance.

3.3. PASSI FALSI CHE POSSONO COMPROMETTERE LA COPERTURA

Soprattutto per quanto riguarda la copertura informatica, è fondamentale che le aziende comprendano che, il loro lavoro non è terminato dopo aver acquistato una polizza informatica (Selby, 2020). L'assicurato deve essere consapevole delle dichiarazioni fatte alla compagnia assicurativa in relazione al suo acquisto e comprendere gli obblighi imposti dai termini e dalle condizioni della polizza, in caso contrario, la copertura potrebbe essere messa a rischio in caso di sinistro.

Alcune delle questioni chiave da tenere a mente sono:

1. dichiarazioni fatte all'assicuratore; si dovrebbe fare molta attenzione nel completare accuratamente una domanda di cyber insurance, che entrerà a far parte della polizza se questa verrà emessa, inoltre eventuali futuri assicuratori possono includere un'approvazione a una nuova polizza informatica che, preveda che le dichiarazioni fatte dall'assicurato, in una precedente domanda, vengano invocate

[43] Si definisce "evento informatico" che richiede un'intrusione nel sistema informatico dell'assicurato da parte di terzi o la divulgazione di informazioni private.

in relazione alla nuova emissione. Saranno probabilmente richiesti input da una sezione trasversale di parti interessate in tutta l'azienda, tra cui la gestione del rischio, legale, risorse umane e tecnologia dell'informazione al fine di fornire risposte corrette alle domande dell'assicuratore. Gli assicuratori possono richiedere al presidente, al CEO e/o al CIO della compagnia di firmare la domanda compilata e di attestare l'accuratezza delle risposte della compagnia. Informazioni imprecise fornite da una società nel processo di candidatura possono compromettere la copertura, se una richiesta di risarcimento viene successivamente presentata nell'ambito della polizza. Ad esempio, XYZ Inc. afferma nella sua applicazione che crittografa debba fornire sempre i dati contenenti informazioni personali identificabili (PII) e un assicuratore emetta una polizza in base alle dichiarazioni di XYZ. Se XYZ dovesse essere violato durante il periodo di polizza, con conseguente furto di informazioni personali non crittografate, la copertura per la sua richiesta potrebbe essere a rischio.

Alcuni assicuratori potrebbero richiedere al potenziale assicurato di fornire informazioni aggiornate prima che venga emessa una polizza, se eventuali risposte nella domanda presentata non risultassero più accurate.[44].

La condizione "assistenza e cooperazione" di una polizza informatica può richiedere espressamente all'assicurato di collaborare con la compagnia assicurativa in qualsiasi indagine ritenga necessaria in merito alla domanda di copertura. La violazione di tali condizioni potrebbe compromettere seriamente la copertura.

2. Esclusioni relative alle risposte sul modulo. Le polizze informatiche possono contenere una "mancata osservanza delle pratiche minime richieste" o un'esclusione analoga. Tali esclusioni si applicano espressamente alle perdite connesse al fallimento dell'assicurato "di attuare continuamente le procedure e i controlli dei rischi identificati nella domanda dell'assicurato".

   Gli assicurati dovrebbero accertarsi che, le risposte nel modulo della polizza rispecchino la verità e garantire che esse rimangano accurate durante la durata della polizza.
3. Avviso delle condizioni di reclamo. Le polizze informatiche contengono

[44] È probabile che questo requisito venga imposto se esiste un divario significativo, di solito superiore a 90 giorni, tra la data della domanda completata e l'emissione della polizza.

abitualmente disposizioni esplicite relative a come e quando un assicurato debba comunicare una richiesta di risarcimento. A seconda della formulazione esatta del contratto, delle circostanze di fatto e della legge applicabile, la mancata osservanza da parte dell'assicurato della condizione di preavviso di una polizza può giustificare il rifiuto dell'assicuratore. Gli obblighi imposti all'assicurato possono variare notevolmente da polizza a polizza, inoltre, altre sezioni della polizza, comprese definizioni e condizioni, possono contenere anche termini che incidono sugli obblighi di preavviso dell'assicurato. Gli assicurati, pertanto, sono invitati a comprendere i requisiti specifici della loro polizza e ad attuare processi interni per identificare le persone implicate dalla polizza e istruirle in anticipo sulle loro responsabilità. Se l'assicurato ha acquistato anche livelli eccedenti di copertura informatica, dovrà rivedere attentamente i requisiti di preavviso in tali polizze.

4. Consenso preliminare e requisiti. Le polizze informatiche possono richiedere all'assicurato di ottenere il consenso dell'assicuratore prima di spendere fondi in relazione a un evento coperto dalla polizza. Ad esempio, alcuni assicuratori richiedono che l'assicurato ottenga il "previo consenso scritto" dell'assicuratore in anticipo, in relazione ai costi sostenuti per rispondere a una richiesta di violazione, reclamo o riscatto, mentre altri consentono flessibilità sul problema. Per un assicurato che affronta una violazione della sicurezza, arresto della rete o attacco ransomware, ottenere il consenso scritto di un assicuratore, prima di affrontare la situazione potrebbe non essere implicito, di conseguenza, si consiglia agli assicurati di prendere nota delle disposizioni del consenso preventivo della loro polizza e di incorporare tali requisiti nei loro piani di risposta agli incidenti e nei programmi di formazione dei dipendenti. Gli assicurati dovrebbero inoltre essere consapevoli del fatto che, alcuni assicuratori informatici impongono l'uso di professionisti preselezionati, inclusi avvocati, specialisti forensi e società di notifica, in caso di incidente coperto. È fondamentale che gli assicurati conoscano i requisiti specifici del loro assicuratore, prima di subire un incidente informatico e spendere fondi per trattenere i fornitori di servizi. Alcuni assicuratori possono consentire all'assicurato di selezionare i propri fornitori di servizi, ma tale questione viene affrontata nelle negoziazioni prima dell'emissione della polizza.
5. Responsabilità assunta in base alle esclusioni contrattuali. Come molte altre polizze assicurative di responsabilità civile, le polizze informatiche di solito

contengono un'esclusione per le responsabilità che, l'assicurato abbia assunto in virtù di un contratto. Sebbene vi siano generalmente eccezioni a tali esclusioni per le passività che, l'assicurato avrebbe anche in assenza di un contratto, alcune importanti e comuni esposizioni informatiche potrebbero rientrare nell'ambito di questa esclusione. Esempi importanti includono accordi di risarcimento con banche in relazione all'uso della carta di pagamento e contratti tra l'assicurato e i suoi partner commerciali in merito ai servizi di gestione dei dati.

È importante sottolineare che, molte politiche contengono ritagli per l'esclusione di determinate esposizioni come multe, spese e costi del settore delle carte di pagamento.

Ai fini della gestione generale del rischio, tuttavia, gli assicurati dovrebbero ben comprendere la portata degli obblighi assunti nell'ambito di contratti che, probabilmente rientreranno nell'ambito di questa esclusione.

6. Disposizioni su fusioni e acquisizioni. Le polizze informatiche, come la maggior parte delle altre forme di polizza, in genere forniscono copertura all'assicurato designato e identificato nella polizza, nonché a qualsiasi sussidiaria dell'assicurato nominato creata alla data di entrata in vigore della polizza. Gli assicuratori generalmente chiedono alle imprese di identificare tutte queste filiali durante il processo di candidatura. Sebbene le società affiliate divulgate possano in genere essere considerate "assicurate", nel momento in cui viene emessa una polizza informatica, la polizza può contenere disposizioni che, specifichino i passi che devono essere compiuti per ottenere copertura per le filiali acquisite, create o per le entità coinvolte in fusioni o consolidamenti durante il periodo della polizza. Le misure che un assicurato deve adottare per garantire la copertura di una nuova controllata variano da polizza a polizza e possono dipendere dai dati finanziari della controllata. Ad esempio, nell'ambito di una polizza informatica, se l'entità acquisita ha entrate superiori al 10% delle entrate annue totali dell'assicurato nominato, esso deve: fornire comunicazione scritta prima dell'acquisizione, ottenere il consenso scritto dell'assicuratore e accettare di pagare qualsiasi premio aggiuntivo richiesto dall'assicuratore.

   Un altro assicuratore richiede ad un assicurato che si fonda con, che acquisisca o crei un'entità con attività superiori al 10% delle attività totali dell'assicurato, di fornire i dettagli completi della transazione non appena possibile.

   L'assicuratore ha il diritto di imporre termini, condizioni e premi aggiuntivi, a sua

esclusiva discrezione[45]. Alla luce dei vari requisiti imposti dai diversi assicuratori, gli assicurati coinvolti in attività di fusione o acquisizione dovrebbero rivedere attentamente le loro cyber policy all'inizio del processo di negoziazione. Le disposizioni pertinenti possono essere trovate in una varietà di sezioni della polizza, a seconda del modulo in questione, anche all'interno delle condizioni, definizioni e sezioni di esclusione.

3.4. IL RUOLO DEL GDPR NELLA CYBER INSURANCE

La copertura assicurativa informatica può coprire qualsiasi cosa, dalla riparazione di software e hardware a seguito di una violazione dei dati, al rimborso di spese legali, spese di pubbliche relazioni e perdita di attività.
Secondo una buona stima, l'ammontare dei premi annuali di assicurazione informatica in Europa potrebbe superare i 2 miliardi di euro entro il 2020 (Lloyds, 2019).
I rischi di conformità al GDPR saranno un fattore determinante: la buona notizia è che le aziende che hanno già sottoscritto una copertura informatica troveranno molti aspetti del GDPR come già gestiti dalle polizze attuali, tuttavia per ogni grande cambiamento nel contesto normativo, permangono alcune incognite.
L'assicurazione informatica copre sanzioni e multe associate alla violazione della privacy e protezione dei dati, eppure, prima di considerare una polizza come buona corrispondenza per i requisiti GDPR è necessario "leggere le scritte in piccolo" (Selby, 2018).

3.4.1. VERIFICA DI COMPATIBILITÀ TRA GDPR E CYBER POLICY

Quando si valuta una copertura assicurativa informatica in relazione al GDPR, bisognerebbe assicurarsi che la polizza sia chiaramente orientata a (Stephen, 2019):

[45] Secondo i termini di una certa polizza, se l'assicurato nominato acquisisce o crea un'altra organizzazione in cui l'assicurato nominato ha un interesse di proprietà superiore al 50%, l'organizzazione è coperta per eventi assicurati che si svolgono dopo la data di acquisizione o creazione, ma solo se l'assicurato designato ha notificato all'assicuratore entro e non oltre 60 giorni dalla data effettiva dell'acquisizione della creazione, insieme a tutte le informazioni che l'assicuratore dovrebbe richiedere. L'assicurato può essere esonerato da tale procedura se, tra l'altro, le entrate lorde della nuova controllata sono pari o inferiori al 10% rispetto a quelle dell'assicurato designato.

- definizione di un regolatore della privacy. Le compagnie di assicurazione spesso includono entità "straniere" o "internazionali" nel loro elenco di regolatori qualificati della privacy. Alcuni saranno più specifici, in particolare, per quanto riguarda il GDPR e includeranno esplicitamente le autorità europee per la protezione dei dati (DPA).

  Questo viene fatto per offrire il conforto all'assicurato che la polizza si occupa del GDPR, in realtà, precisare i regolatori europei, non è di solito un cambiamento sostanziale.
- Distinzione delle tante sfaccettature del termine "violazione della privacy". Il GDPR copre una serie molto ampia di problemi di privacy, precisando inoltre le modalità di gestione dei dati nei vari stadi.

  Gli assicuratori stanno già espandendo la propria copertura assicurativa per far fronte a questi nuovi tipi di esposizioni, tuttavia, anche le polizze assicurative più aggiornate potrebbero non coprire tutte le violazioni della privacy del GDPR. Ad esempio, è improbabile ottenere una copertura per la mancata designazione di un responsabile della protezione dei dati, requisito GDPR per le organizzazioni coinvolte nel trattamento su larga scala di questi.
- Sede più favorevole per sanzioni e multe. Le penalità e le multe del GDPR si applicano alle imprese con sede nella UE e a quelle che trattano con clienti della UE. La disposizione della sede più favorevole è la sezione di una polizza assicurativa informatica che, segnala l'intenzione di un assicuratore di pagare una multa o sanzione quando possibile, in altre parole, si terrà conto di tutte le sedi ragionevoli prima di decidere se una sanzione o un'ammenda sia assicurabile. Questi fattori includono la posizione dell'evento, la sede della società o la sede in cui è incorporata l'attività.

  Le norme non hanno sempre incluso questa disposizione, tuttavia, un numero crescente di assicuratori sta dimostrando la propria disponibilità a farlo, il che è cruciale per la conformità al GDPR.
- Il limite è sufficiente? Le penalità e le multe del GDPR superano il 4 % delle entrate globali di un'azienda che, per le grandi società, può tradursi in miliardi di euro. Naturalmente i regolatori sono ragionevoli, riservando la massima pena per le violazioni significative e ripetute nel tempo.

È comunque impossibile essere completamente sicuri del modo in cui i regolatori valuteranno ogni violazione e quindi determineranno la sanzione appropriata, quindi le grandi aziende dovrebbero rivedere i limiti della propria copertura assicurativa informatica, così da giudicare come essa si regolerebbe contro una sanzione massima.

- Assicurazione informatica per fornitori. Le polizze informatiche non sono obbligatorie in nessuna parte del mondo, eppure gli obblighi contrattuali e le considerazioni sulla continuità aziendale dovute al GDPR possono costringere le imprese all'interno dell'UE non solo a stipulare una copertura assicurativa informatica, ma anche a chiedere ai loro venditori locali e internazionali di fare altrettanto.

  Se un fornitore viola le leggi sulla privacy della UE, l'entità dell'ammenda potrebbe costringerlo a cessare l'attività, impattando così in maniera negativa sulle operazioni delle società che riforniscono.

  È quindi fondamentale garantire che, tutti i fornitori critici dispongano di una copertura assicurativa informatica compatibile con la conformità al GDPR, in modo da facilitare la continuità aziendale e il processo di ripristino in caso di emergenza.

È chiaro che il GDPR guiderà alcuni cambiamenti nelle modalità e motivazioni per cui le aziende sottoscriveranno la cyber insurance; come con qualsiasi nuova legge, ci saranno alcune situazioni impreviste, ma la chiave per mantenere sana un’attività è assicurarsi di aver coperto tutte le possibili situazioni rischiose e prepararsi al meglio per le incognite (Stephen, 2019).

Capitolo 4

4. LA CYBER INSURANCE: MODELLIZZAZIONE E PRICING

4.1. INTRODUZIONE ALLA COSTRUZIONE DEL MODELLO DEL CYBER SECURITY RISK

La cyber insurance viene spesso definita come l'ultimo mezzo per gestire i residui dei rischi della sicurezza IT, ma il calcolo del premio è ancora una domanda aperta (Maochao e Lei, 2017).

La segnalazione delle perdite finanziarie, a causa di violazioni nella sicurezza delle informazioni, offre una visione d'insieme della gravità del problema, poiché esse possono comportare perdite milionarie a causa di costi diretti, come la perdita delle entrate, la perdita di produttività e quella derivante da cause legali, nonché perdite più immateriali come la perdita di avviamento commerciale, di reputazione e di opportunità (Biener et al., 2014).

Il Crime and Security Survey (Richardson, 2008) osservò che la maggior parte delle organizzazioni utilizza strumenti di sicurezza: il 97% software antivirus, il 94% firewall e il 69% sistemi di rilevamento delle intrusioni; nonostante questo, le violazioni e le perdite rimangono elevate.

È difficile per i responsabili della sicurezza di qualsiasi organizzazione conoscere ed eliminare tutti i punti di vulnerabilità in un sistema IT (ad esempio, creare un sistema infallibile) e un hacker ha bisogno di uno solo di questi punti da poter sfruttare (Anderson, 2001).

Riconoscendo che, l'eliminazione totale del rischio è quasi impossibile, il National Institute of Standards and Technology (NIST) raccomanda diverse tecniche di mitigazione, basate su controlli tecnici e non tecnici, che comprendono: l'assunzione del rischio, la prevenzione per evitarlo, la limitazione, la pianificazione, la ricerca, il riconoscimento e il trasferimento del rischio (Stoneburner et al., 2002).

Ci si concentra così sul trasferimento del rischio come strumento che, minimizza alcune delle perdite finanziarie per le imprese (utilizzando altre opzioni per compensare la

perdita, come l'acquisto di un'assicurazione).

I tradizionali prodotti assicurativi coprono proprietà tangibili ma non coprono risorse come dati e informazioni; invece la cyber assicurazione è progettata appunto per coprire principalmente i beni immateriali che l'assicurazione tradizionale non copre. Tali polizze assicurative aiutano a proteggere da perdite dovute ad attacchi informatici, violazioni della sicurezza della rete, gli hacker e le spese conseguenti.

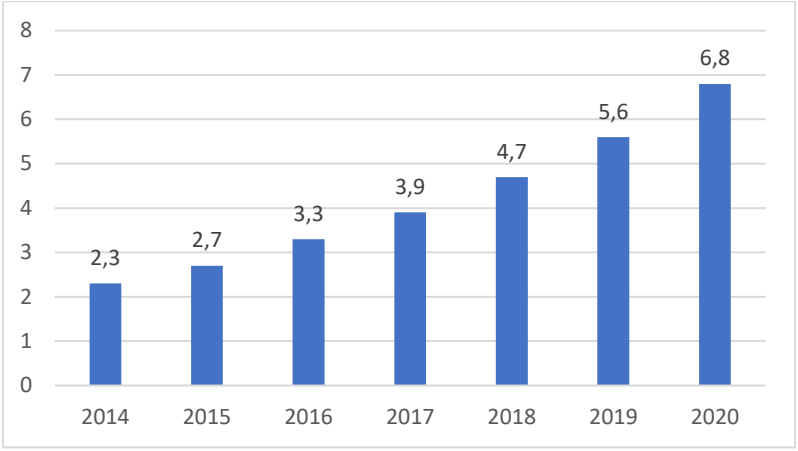
Il mercato cyber assicurativo si è sviluppato con l'avvento e la diffusione di Internet nelle attività commerciali; sebbene la copertura contro la criminalità informatica sia apparsa per la prima volta negli anni '70, essa era principalmente legata all'ambito bancario (Majuca, 2006).

Le aziende stanno cercando una copertura per il valore della perdita dei dati, della perdita di entrate conseguente, delle entrate perse a causa di tempi di inattività, le spese legali per danni a terzi, il costo di gestione delle crisi, la notifica, il monitoraggio del credito e il ripristino dopo una violazione dei dati, le multe regolamentari e le penalità (Betterley, 2010).

I premi variano a seconda della situazione e la quantità di copertura può variare da poche migliaia di euro per quella base per piccole imprese (meno di 10 milioni di euro di entrate) a centinaia di migliaia di euro per le grandi società che, desiderano una protezione completa. Si stima che il premio lordo annuale della cyber insurance sarà di 6.8 miliardi di euro nel 2020 rispetto ai 5.6 nel 2019 (Rudden, 2019).

Sebbene le società di assicurazione forniscano questi tipi di prodotti, l'accuratezza dell'ammontare del premio è ancora una domanda aperta (Gordon et al., 2003); i premi dipendono dal tipo e dall'esposizione al cyber risk della singola impresa e possono variare sostanzialmente a seconda del fornitore dell'assicurazione. Per affrontare questo, gli accademici hanno sostenuto un consistente e innovativo modello di tariffazione della cyber assicurazione, al fine di stimolare una crescita del mercato (Baer and Parkinson, 2007).

Figura 4.1: La crescita del cyber insurance market dal 2014 al 2020 (ultimi due anni stimati).



Fonte: Advanced Cyber risk management report (Yeo, 2019).

I contributi alla modellizzazione del rischio di cyber security in letteratura sono ampiamente descrittivi; questo tipo di rischio, è molto diverso dai rischi tradizionali coperti dall'assicurazione per la responsabilità civile.

La proprietà significativa che distingue il rischio cibernetico dal rischio convenzionale è l'interconnessione delle risorse della tecnologia dell'informazione e della comunicazione (TIC), pertanto, l'analisi del rischio e delle relative perdite potenziali, deve tener conto della tipologia della rete. Inoltre, a causa del potenziale dirottamento di risorse TIC, le fonti benigne (ad es. i computer) possono diventare minacce per altre fonti. Tradizionalmente, i prezzi dei prodotti assicurativi, si basano su tabelle attuariali costruite su documenti storici, ma a differenza delle polizze assicurative tradizionali, la cyber insurance non ha sistemi di punteggio standard o tabelle attuariali (Maochao e Lei, 2017).

I rischi per la cyber security sono relativamente nuovi e i dati attinenti a violazioni e perdite di sicurezza non esistono o esistono solo in quantità minori e questa difficoltà può essere ulteriormente esacerbata dalla riluttanza delle imprese a rivelare i dettagli delle violazioni della sicurezza, dovuta alla perdita di quote di mercato, di reputazione, ecc.

Gli assicuratori tendono ad aumentare i premi per le società più grandi e la copertura può essere limitata e molto costosa per le società senza una buona protezione.

La letteratura rivela diversi sforzi per studiare il rischio di sicurezza informatica attraverso modelli matematici, ad esempio, Gordon et al. (2003) discutono di un quadro generale in materia di pricing e questioni di selezione avversa dell'assicurazione informatica e propongono un piano decisionale in quattro fasi per il rischio informatico (Maochao e Lei, 2017).

Bohme e Kataria (2006) considerano la correlazione tra i rischi informatici e usano la distribuzione beta-binomiale[46] e un modello di rischio latente ad un fattore con scopo di modellizzazione, discutendo in modo particolare della correlazione tra il rischio di sicurezza informatica all'interno di un'azienda e il rischio a livello globale.

Bohme e Schwartz (2010) esaminano un quadro per la gestione delle proprietà specifiche del cyber security risk, compresa la sicurezza interdipendente, il rischio correlato e l'asimmetria delle informazioni. Essi presentano inoltre un sondaggio sui modelli esistenti di assicurazione relativi alla sicurezza informatica, in cui viene discussa una discrepanza tra argomentazioni informali a favore dell'assicurazione informatica, come strumento per migliorare la sicurezza della rete.

Un breve approccio bayesiano viene proposto da Mukhopadhyay et al. (2006) per modellare il rischio di sicurezza informatica. Essi utilizzano la copula gaussiana multivariata per modellare la distribuzione congiunta e la distribuzione condizionale di ciascun nodo sulla rete e i premi sono calcolati in funzione del valore atteso della gravità del sinistro.

Herath e Herath (2011) propongono un modello attuariale basato sulle copule per la determinazione del prezzo del rischio di sicurezza informatica in cui modellano tre variabili di rischio: il verificarsi dell'evento, il tempo, e l'importo del pagamento. I premi per le perdite subite a causa di attacchi epidemici sono calcolati utilizzando tre tipi di modelli di polizza assicurativa: polizza con zero franchigia, la polizza con franchigia e la polizza con coassicurazione[47] e i limiti.

Schwartz e Sastry (2014) presentano un quadro per la gestione del rischio di sicurezza informatica in una rete interdipendente su larga scala, considerando gli assicuratori informatici come attori strategici, giungendo così alla soluzione per la sicurezza ottimale dell'utente in ambienti con e senza assicuratori informatici.

Yang e Lui (2014) usano un gioco bayesiano per modellare l'investimento in sicurezza informatica in cui viene considerato l'effetto dell'esternalità della rete; viene mostrato che

[46] La beta-binomiale è una distribuzione di probabilità discreta vista come una generalizzazione della distribuzione binomiale. Descrive il numero di successi su *n* esperimenti indipendenti, ma, contrariamente alla distribuzione Binomiale, la probabilità di successo non è un parametro fisso ma un valore distribuito come una variabile casuale Beta. Si tratta infatti di una mistura di Binomiali il cui il parametro assume distribuzione Beta.

[47] La coassicurazione è quel contratto assicurativo stipulato da più compagnie assicuratrici a copertura del medesimo rischio per quote predeterminate, dove, in caso di sinistro, le compagnie assicuratrici sottoscriventi sono tenute a corrispondere l'indennizzo in proporzione alla quota assicurata (assicurazione.it)

i nodi con più gradi[48] hanno maggiori probabilità di essere infettati e di essere influenzati dalle decisioni altrui.

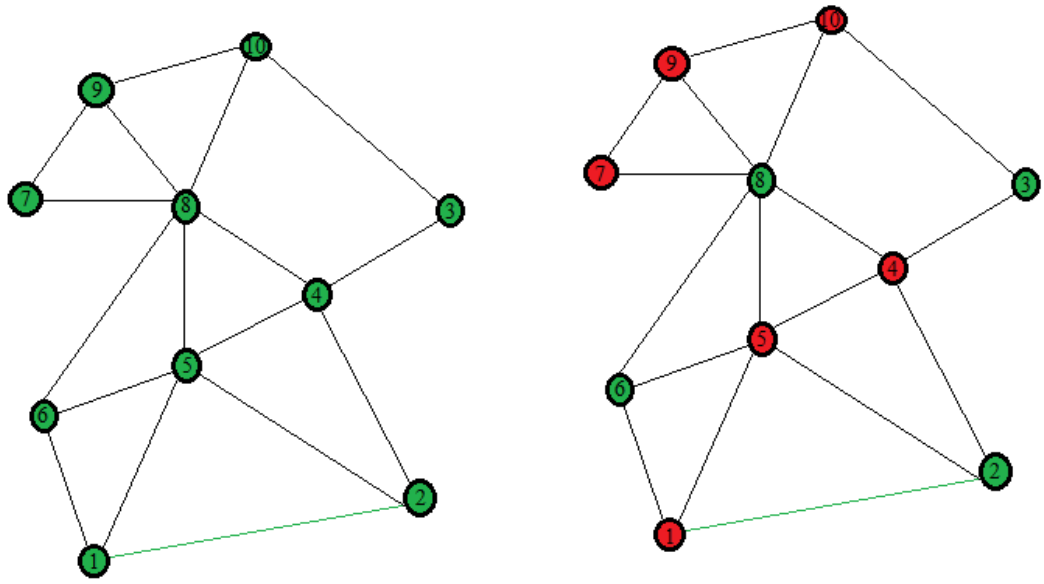
Si può fare riferimento a Kosub (2015) ed Eling e Schnell (2016) per revisioni complete sulla modellizzazione del rischio di sicurezza informatica e sulla sua gestione.

Il lavoro di Maochao e Lei (2017) è diverso da altri in letteratura nei seguenti aspetti: essi utilizzano processi stocastici (Markov e non-Markov) per descrivere le dinamiche della diffusione dell'epidemia nel tempo, mentre la maggior parte dei modelli delle opere sopra menzionate sono statici. Essi propongono di usare le copule per catturare la dipendenza tra le distribuzioni del tempo all'infezione, mentre in letteratura si presume che, le infezioni siano indipendenti nel tempo; suggeriscono inoltre di utilizzare la simulazione Monte Carlo per valutare il livello di sicurezza delle reti, che include: il numero di incidenti, le probabilità di infezione dei nodi e le perdite totali.

Per esempio, si supponga che un'azienda le cui risorse TIC, abbiano la struttura di rete descritta dalla Figura 1 desideri acquistare la cyber insurance, dove i nodi rappresentano computer (e/o server). Si è visto al momento t_1 che nessuno dei computer è infetto, tuttavia, al momento t_2, sei computer sono infetti. Per una compagnia assicurativa che, vuole offrire polizze assicurative sulla cyber security il passo fondamentale è comprendere l'evoluzione della diffusione dell'epidemia sulla rete, poiché essa causerà perdite a livello pratico; è anche importante conoscere l'ammontare totale della perdita durante un determinato periodo di tempo, poiché i premi sono determinati in base alle perdite.

[48] Il grado di un nodo è dato dal numero di archi incidenti ad esso.

Figura 4.1: Epidemia cibernetica che si diffonde in rete per un'impresa con 10 computer/server al momento t1 e t2, con i punti rossi che rappresentano i computer infettati.



Fonte: Cybersecurity Insurance: Modeling and Pricing (Maochao e Lei, 2017).

4.2. LA DISTRIBUZIONE DEL CYBER SECURITY RISK

Si supponga che un'azienda abbia una rete che potrebbe essere descritta come un grafico non orientato[49] $\Gamma = (V; \mathbb{E})$, dove V è il nodo impostato ed $\mathbb{E}$ è il bordo impostato (Maochao e Lei, 2017). Si noti che Γ riassume la struttura di rete in base alla quale avvengano gli attacchi informatici (ad esempio diffusione di malware), in cui $(u, v) \in \mathbb{E}$ implica che, i nodi u e v possano attaccarsi a vicenda (grafico non orientato). In linea di massima, Γ può variare da un grafico completo (cioè qualsiasi u $\in V$ può attaccare qualsiasi $v \in V$) a qualsiasi struttura grafica specifica. Indicando con $A = (a_{vu})$ la matrice di adiacenza di Γ, dove $a_{vu} = 1$ se e solo se $(u, v) \in \mathbb{E}$, e $a_{vu} = 0$ in caso contrario, si noti che l'impostazione del problema implica naturalmente $a_{vv} = 0$. Indicando con $deg\ (v)$ il grado del nodo v e $N = | V |$ il numero totale di nodi, è possibile constatare che, il nodo $v \in V$ è sicuro (ma vulnerabile agli attacchi) o infetto (e può attaccare altri nodi) in qualsiasi momento t =

[49] Due vertici *u, v* connessi da un arco *e* prendono il nome di estremi dell'arco, dove lo stesso arco viene anche identificato con la coppia formata dai suoi estremi (u,v). Se E è una relazione simmetrica allora si dice che il grafo è non orientato (o indiretto).

0,1, ⋯. Lo stato di questa rete al momento t può essere rappresentato come

$$(I1(t),\cdots,IN(t));$$

dove

- $Iv\,(t) = 1$ rappresenta il nodo v nello stato di infezione al momento t, mentre
- $Iv\,(t) = 0$ indica che il nodo v è sicuro al momento t.

Il vettore di probabilità di infezione è indicato da

$$\boldsymbol{p}T\,(t) = (p1\,(t), \cdots, pN\,(t)); \tag{4.1}$$

dove

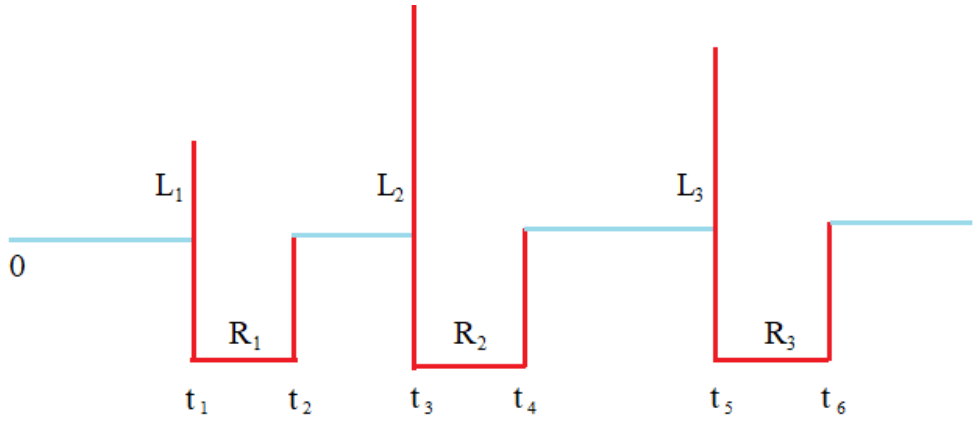
- $pj\,(t) = P\,(Ij = 1)$, per $j = 0,1, \cdots, N$.

Consideriamo due minacce affrontate da ciascun nodo:

1. minacce esterne alla rete (ovvero, il nodo v è infetto perché viene attaccato o il suo utente visita un sito Web dannoso);
2. minacce all'interno della rete (ovvero, il nodo v è infetto, quindi attacca i suoi vicini).

Sono stati fatti molti lavori per modellare l'epidemia che si sta diffondendo sulla rete informatica.

Figura 4.2: Cybersecurity risk per il nodo v.



Fonte: Cybersecurity Insurance: Modeling and Pricing (Maochao e Lei, 2017).

A scopo illustrativo, considerare lo scenario in Figura 4.2. Il nodo v è sicuro al momento $T = 0$ e la prima infezione si verifica al momento $T = t_1$. L'infezione comporterebbe due

tipi di perdite:

1. perdita causata dall'infezione (ad esempio informazioni rubate, dati danneggiati, registrazioni esposte e spese legali di prima parte);
2. perdita causata dal ripristino del nodo.

Il primo tipo di perdita è modellato da un costo casuale $\eta_v(L_{v,1})$, dove $L_{v,1}$ indica la perdita di informazioni (ad es. dati danneggiati) e può anche essere utilizzato per modellare il costo legale di prima parte. Il secondo tipo di perdita è correlato alla durata dell' *out of service* (o in riparazione) ed è modellato da una funzione di costo $C_v(R_{v,1})$, dove $R_{v,1}$ è la durata del' out of service. Al momento $T = t_2$, il nodo v è sicuro, ma vulnerabile agli attacchi e verrà nuovamente infettato al tempo t_3 e ancora in t_5. Pertanto, per il nodo v, la perdita cumulata nel tempo t può essere rappresentata come:

$$S_v(t) = \sum_{i=1}^{M_v(t)} [\eta_v(L_{v,i}) + C_v(R_{v,i})]; \tag{4.2}$$

dove

- $\eta_v(\cdot)$ rappresenta il costo dovuto all' infezione;
- $C_v(\cdot)$ rappresenta la funzione di costo associata a
- $R_{v,i}$ che è la durata del fuori servizio.

Per ogni nodo v, infatti, si tratta un processo di ricompensa del rinnovo[50]. La perdita totale affrontata dall'azienda durante $(0, t)$ è

$$S(t) = \sum_{v=1}^{N} S_v(t) = \Sigma_v^N \sum_{i=1}^{M_v(t)} [\eta_v(L_{v,i}) + C_v(R_{v,i})]; \tag{4.3}$$

dove

- $Mv\,(t)$ è il numero totale di infezioni del nodo v fino a tempo t.

L'equazione (4.1) mostra che la quantità chiave è il vettore di infezione $(I_1(t),\cdots,I_N(t))$, richiedente la teoria epidemica[51].

[50] In un processo di ricompensa di rinnovo, ogni intervallo di tempo è associato a una variabile casuale che è generalmente considerata la ricompensa associata a quell'intervallo

[51] Nella sua versione più semplice, la teoria epidemica considera tre variabili: agente, ospite e ambiente. Ognuno di queste ha molte componenti, tuttavia le interazioni ospite-agente variano notevolmente e le

4.3 IL MODELLO MARKOV[52]

Il processo di Markov viene utilizzato per modellare il cyber security risk; prima di tutto si suppone che, il processo di recupero di qualsiasi nodo infetto v si distribuisca come una Poisson con parametro δv (Maochao e Lei, 2017).
Il processo di infezione per collegamento è anch'esso assimilabile ad una Poisson con parametro β a causa dei vicini infetti all'interno della rete; qualsiasi nodo potrebbe diventare infetto con probabilità determinata dal parametro di una distribuzione di Poisson ϵv a causa della minaccia esterna alla rete. Si presume che i processi di infezione e i processi di recupero siano indipendenti.
Questo modello, infatti, è noto in letteratura come modello SIS o SIR, tuttavia il modello epidemico basato sui gradi non può catturare propagazioni epidemiche in reti specifiche. Per ogni nodo v, i processi di infezione e recupero formano il seguente processo di Markov:

$$I_v(t) = 0 \to 1 \text{ al tasso } \beta \sum_{J=1}^{n} a_{vJ} I_J(t) + \epsilon_v;$$
$$I_v(t) = 1 \to 0 \text{ al tasso } \delta_v. \tag{4.4}$$

Il seguente risultato fornisce un limite superiore dinamico per le probabilità di infezione, che può essere utilizzato come stima per le infezioni sulla rete (Maochao e Lei, 2017).

Teorema 4.1 Sia Q = diag(($\beta\delta v$) / ($\delta v + \epsilon v$)) A − diag ($\delta v + \epsilon v$). Quindi il limite superiore dinamico per la probabilità di infezione è

$$p^*(t) = e^{Qt} p^*(0) + Q^{-1}(e^{Qt} - 1)\epsilon, \tag{4.5}$$

dove

variazioni delle condizioni ambientali le influenzano in innumerevoli modi. La teoria epidemica è quindi estremamente complessa, coinvolgendo la matematica stocastica avanzata.

[52] Per il modello non-Markov, invece, si assume che per ogni nodo v, esista Dv, che infetto da vicini e da attacchi tramite collegamenti, i cui tempi di infezione sono modellati come variabili casuali ($Yv1,\cdots,YvDv$) con la stessa distribuzione marginale F. Il tempo di infezione da parte delle minacce al di fuori della rete è modellato dalla variabile casuale Zv con distribuzione Gv.

- $\epsilon^T = (\epsilon_1, \dots, \epsilon_n)$;
- $e^{Qt} = \sum_{k=1}^{\infty} \frac{Q^t k^t}{k!}$.

4.3.1 SIMULAZIONE E PRICING

Prima di procedere con la simulazione e pricing si supponga che per un nodo v, la ricchezza (o informazione) iniziale sia e_v. Poiché l'evento di infezione potrebbe non comportare una perdita totale di informazioni, supponiamo che la perdita del nodo v sia distribuita in base alla distribuzione beta con funzione di densità:

$$f_{L_v}(x) = \frac{1}{\omega_v^{a+b-1}} \frac{1}{B(a,b)} x^{a-1}(\omega_v - x)^{b-1}; \qquad 0 \leq x \leq \omega_v \tag{4.6}$$

dove

- $a, b > 0$ sono parametri;
- B è la funzione beta.

Le funzioni di costo sono definite come

$$\eta_v(l_v) = cl_v, \quad C_v(r_v) = C_1\omega_v + C_2 r_v; \tag{4.7}$$

dove

- C indica la percentuale di costo dovuta all'infezione;
- C_1 rappresenta la percentuale di costo in base al valore iniziale;
- C_2 rappresenta la percentuale di costo del processo di recupero.

Si vede che la funzione di costo definita in Eq. (4.7) dipende non solo dalla durata dei tempi di inattività, ma anche dalla salute del nodo. Valutando un contratto assicurativo di un anno e considerando due principi di premio, il primo è il principio della deviazione standard:

$$H(x) = E[X] + \lambda\sqrt{Var(X)}; \tag{4.8}$$

dove

- $\lambda > 0$ è l'ammontare del rischio.

Il secondo è il principio di utilità equivalente, in cui il premio H (X) risolve l'equazione:

$$u(\omega_v) = E\big[u\big(\omega_v - X + H(X)\big)\big], \tag{4.9}$$

dove

- u è una funzione di utilità crescente e concava di salute;
- ω è lo stato di salute iniziale.

La funzione costante e relativa di utilità avversa al rischio, che è comunemente usata in letteratura, è rappresentata invece così:

$$\begin{cases} \frac{\omega^{1-\gamma}}{1-\gamma} \; se \; \gamma \neq 1 > 0 \\ log(\omega) \; se \; \gamma = 1 \end{cases} ; \tag{4.10}$$

dove

- γ è il parametro di grado di avversione al rischio.

4.4 ESTRAZIONE DEL CYBER RISK TRAMITE PRODOTTI FINANZIARI STRUTTURATI

L'idea alla base di questo approccio è che, se i mercati sono efficienti, i prezzi di mercato riflettono correttamente le aspettative, quindi, partendo dal presupposto che un decision maker (DM), un governo, o una compagnia assicurativa, siano interessati a ottenere informazioni sui futuri rischi informatici, esse possano quindi essere utilizzate per valutare i prodotti assicurativi o eventualmente vendute a terzi (Verlaine, 2020).
Come valutare quindi queste informazioni? La questione è stata affrontata da Ganuza e Penalva (2010), Azrieli e Lehrer (2008), e da Cabrales et al. (2013).
Quest'ultimo suggerisce che, la misura generale del valore delle informazioni per la maggior parte dei decisori con diverse avversioni al rischio può essere valutata mediante una riduzione dell'entropia (misura d'incertezza) fornita dalle stesse informazioni (Cabrales et al., 2013). Questo approccio non può essere replicato direttamente per i prodotti finanziari indicizzati al rischio cibernetico, ma un approccio simile può essere sviluppato portando a sostenere dal punto di vista statistico una certa somiglianza con i rischi di credito, inoltre le distribuzioni del cyber risk sembrano avere una coda pesante

e possono essere modellate con la teoria del valore estremo (Zhan et al., 2015).

Backus et al. (2011) sviluppano un modello strutturale per valutare i rischi estremi e catastrofi, che sembra potenzialmente adattato per catturare i rischi informatici estremi; questo è costituito da due componenti: una componente distribuita come una normale per i rischi standard e una componente di salto, che può essere calibrato per diversi livelli di rilevanza e intensità. Gli swap di eventi informatici basati sul modello di credit default swap potrebbero essere utilizzati per estrarre il premio per il rischio di un portafoglio di attività sottostanti soggette a rischi informatici. Supponendo le aspettative e l'efficienza razionali, questo premio è quindi la migliore stima possibile delle perdite attese a causa dei rischi informatici, anche se non è possibile tenere in considerazione i rischi di correlazione tra imprese; devono essere utilizzati prodotti finanziari più avanzati, chiamati prodotti di correlazione e quello più adatto è il CDO (collateralized debt obligation).

Dal momento che tali prodotti hanno diversi livelli di copertura assicurativa per diversi livelli di significatività della perdita, i premi di rischio per le tranche indicano potenzialmente le perdite previste per ciascuna di esse quindi, strutturando i prodotti in tranche sempre più fini, è possibile estrarre una stima sempre più accurata della distribuzione delle perdite. Ogni perdita all'interno di una determinata tranche può essere vista come una perdita in un determinato stato di rischio e l'approccio del prezzo dello stato Arrow-Debreu può essere applicato insieme all'approccio entropico per valutare le informazioni potenziali in questa distribuzione. Tale approccio potrebbe essere implementato utilizzando l'approccio dei prezzi CDO, per estrarre le perdite attese tramite tranche, dati i prezzi osservati; se esistesse un mercato di tali prodotti strutturati, i prezzi di mercato osservati rifletterebbero correttamente le perdite attese, a condizione che il mercato sia più o meno efficiente.

La distribuzione della perdita attesa estratta, tuttavia si basa su una distribuzione di probabilità neutrale al rischio e può essere confrontata con la distribuzione di probabilità storica stimata dai dati passati. Queste informazioni possono essere utilizzate per valutare il kernel dei prezzi e il valore di informazione attraverso una riduzione dell'entropia come in Cabrales et al. (2013).

4.4.1 IL VALORE DELLE INFORMAZIONI

Da un punto di vista economico, il valore delle informazioni in generale dipende da come quelle nuove riducono l'incertezza relativa agli eventi, da chi le utilizza e quali siano le quelle precedenti e la sua avversione al rischio (Verlaine, 2020). È quindi importante distinguere le informazioni private rispetto a quelle pubbliche: le prime sono detenute da singoli soggetti, mentre l'informazione pubblica è nota al mercato.

Un broker di informazioni potrebbe quindi creare un mercato finanziario per i prodotti informatici strutturati insieme ad altre fonti di informazione e a condizione che il mercato sia efficiente, fornirà le migliori aspettative possibili per i rischi e i prezzi.

Il mercato del cyber risk deve affrontare gli stessi problemi del mercato dei crediti strutturati standard, vale a dire la definizione di eventi, l'incertezza delle perdite quando si verifica l'evento e la correlazione tra eventi.

Se ci concentrassimo più specificamente sul valore delle informazioni per i decisori, sorge un leggero problema: un tipico broker di informazioni che, vorrebbe misurare il valore delle informazioni per i decisori che sono disposti ad acquistarle, deve conoscere l'avversione al rischio e le informazioni private di cui dispone questo decisore. La domanda fondamentale e generale si interroga su quando un'informazione sia più preziosa per un decisore rispetto a qualsiasi altra informazione.

Blackwell (1953) fu il primo ad affrontare il problema della classificazione delle strutture informative, consistenti in un insieme di "segnali" che indicano la probabilità degli eventi. Il suo teorema afferma che la struttura di informazioni più preziosa è quella che fornisce la massima utilità prevista per qualsiasi problema decisionale. Questo approccio, tuttavia, non può classificare completamente le strutture informative.

Cabrales et al. (2013) suggeriscono che la misura generale del valore delle informazioni per la maggior parte dei decisori con diverse avversioni al rischio è fornita da una riduzione dell'entropia fornita dalle informazioni[53]. Più formalmente, Cabrales et al. (2013) considerano la seguente entropia di Shannon (1984):

$$H(q) = -\sum_{k\in K} q(k)\, ln\big(q(k)\big); \tag{4.11}$$

dove

[53] Si immagini per esempio un decisore che si trova ad affrontare l'incertezza riguardo agli eventi futuri. L'entropia è una misura dell'incertezza in una distribuzione che ha valore 0 quando non c'è incertezza o un valore positivo altrimenti.

- $q \in \Delta(K)$ è una distribuzione di probabilità su un insieme di stati $k \in K$.

Se considerassimo un DM con convinzioni *q*, l'entropia di q indicherebbe l'incertezza sugli stati di natura detenuti dal DM. L'entropia è massima quando la distribuzione è uniforme e ogni stato ha la stessa probabilità: quando c'è piena incertezza il valore delle informazioni è più alto, mentre è al minimo quando uno degli stati si verificherà sicuramente[54].

Cabrales *et al*. (2013) mostrano che il valore di una struttura informativa a può essere ricavato attraverso la riduzione prevista dell'entropia, dopo l'osservazione di un segnale *s*. Si assuma che il segnale dell'agente sia *s* con probabilità $p_a(s)$ e la probabilità posteriore su *K* dopo il segnale *s* sia q_a^S, la cosiddetta informatività dell'entropia viene valutata in base alla prevista riduzione dell'entropia per un DM con p informazioni preliminari *p* e tenendo conto dei segnali *s*.

$$I(a) = H(p) - \Sigma_s p_a(s) H(q^s a) \tag{4.12}$$

Si noti che $I(a)$ dipende dalle informazioni del DM prima del segnale p e della struttura informativa a. Data una p precedente , l'indice $I(a)$ definisce un ordinamento completo delle strutture informative. L'informazione ha senso solo quando gli eventi futuri non sono noti con certezza, il decisore acquista quindi le informazioni solo quando vi è incertezza e quando esse permettono di ridurla.

4.4.2 MERCATI EFFICIENTI E STATE PRICE

È possibile inoltre, sviluppare interessanti approcci sulla base dell'efficienza dei mercati[55] così da creare un collegamento tra quelli che sono chiamati i prezzi di Arrow-Debreu

[54] Quando si verifica sicuramente uno stato, l'informazione non ha alcun valore

[55] L'ipotesi dell'efficienza dei mercati sostiene che le informazioni sui prezzi delle attività finanziarie sono rapidamente integrate nei prezzi delle stesse attività. Formalmente, qualsiasi prezzo in qualsiasi momento è dato dalla migliore aspettativa possibile fornita dal set di informazioni disponibili. La migliore aspettativa possibile si chiama Rational Expectation e riflette l'idea che in media gli investitori si aspettino correttamente valori futuri di variabili casuali. Nella letteratura empirica sulla finanza, esistono diversi set di informazioni considerati: prezzi passati nei mercati finanziari, le informazioni pubblicamente disponibili e le informazioni private. Le informazioni disponibili al pubblico sono quelle fornite dalle istituzioni pubbliche come gli istituti statistici, mentre le informazioni private sono quelle detenute da singole aziende o individui.

State[56] (Debreu 1959, Arrow 1964) che, possono essere utilizzati per estrarre le probabilità e le valutazioni soggettive dei rischi attesi dai mercati finanziari. Si ricorre a tali probabilità per valutare i beni e avere così una stretta relazione con l'entropia.
Le applicazioni relativamente recenti di tali tecniche sui prodotti finanziari strutturati e sulle cosiddette obbligazioni di catastrofe economica (Coval *et al*. 2009) forniscono la possibilità di sviluppare i prodotti strutturati indicizzati al rischio cibernetico e utilizzare le informazioni di alcuni di quei prodotti per valutare i rischi e le informazioni. Un mercato del genere non sembra ancora esistere.
La letteratura sull'estrazione dei rischi di catastrofe dalle opzioni sull'indice azionario viene utilizzata per ottenere informazioni sulla distribuzione del rischio informatico dai derivati e dai prodotti strutturati. Tali opzioni forniscono le prove su come gli operatori di mercato stabiliscano il prezzo per gli eventi estremi, indipendentemente dal fatto che si verifichino o meno nel set di dati. È anche interessante evidenziare l'importanza della nozione del kernel[57] dei prezzi, uno strumento di determinazione dei prezzi in ambito finanziario e il collegamento creato con l'entropia.

4.4.3 CYBER RISK E DISTRIBUZIONI DI VALORI ESTREMI

Zhan *et al*. (2013) hanno usato la *grey box prediction* per prevedere il tasso di attacco informatico, ovvero il numero di attacchi per unità di tempo. *I* grey box model prendono in considerazione le proprietà statistiche esibite dai dati, cosa che non fanno i *black box model*. L'approccio del modello *grey box* potrebbe apparentemente prevedere gli attacchi informatici con un'ora di anticipo con una precisione compresa tra il 70% e l'80%; essi

[56] Hanno suggerito che, se i mercati contingenti in cui potrebbero essere scambiate le attività dipendenti da stati futuri dell'economia, allora l'incertezza potrebbe essere scambiata aumentando così l'efficienza dei mercati. Un titolo, tuttavia assume valori diversi in diversi stati dell'economia o del mercato e non può isolare diversi stati; ciò ha portato al concetto di titoli di Arrow-Debreu che, pagano 1 dollaro in un particolare stato dell'economia e 0 altrimenti. Lo stato dell'economia è generalmente una variabile di interesse che riflette gli stati da migliori a peggiori per il decisore.

[57] Il termine kernel è un termine matematico usato per rappresentare un operatore, mentre il termine fattore di sconto stocastico ha radici nell'economia finanziaria ed estende il concetto del kernel per includere gli aggiustamenti per il rischio. I kernel dei prezzi hanno numerosi usi nell'ambito della matematica finanziaria ed economia, ad esempio, i kernel di determinazione dei prezzi possono essere utilizzati per produrre quelli delle richieste potenziali. Se dovessimo conoscere i prezzi attuali di un insieme di titoli, oltre ai futuri profitti, un kernel di valutazione positivo o un fattore di sconto stocastico fornirebbe un mezzo efficiente per produrre prezzi di rivendicazione contingenti ipotizzando un mercato privo di arbitraggi. Questa tecnica di valutazione è particolarmente utile in un mercato incompleto o in un mercato in cui l'offerta totale non è sufficiente a soddisfare la domanda.

notano inoltre che gli errori di previsione possono essere attribuiti all'incapacità di prevedere grandi tassi di attacco, constatando che questo fenomeno è dovuto a valori estremi, modellabili con la teoria degli stessi (EVT).
Secondo gli autori, la previsione di attacchi informatici non è stata affrontata in letteratura a causa di:

- la regola empirica secondo cui i rischi informatici sono imprevedibili;
- la mancanza di dati reali;
- la mancanza di modelli di previsione facilmente utilizzabili.

Essi sottolineano inoltre che la metodologia della grey box, insieme all'approccio EVT, consente un'elevata precisione della previsione del tasso dei cyber attack. Nel loro caso, valori estremi indicano un tasso di attacco elevato, al di sopra di una certa soglia. Al fine di comprendere il comportamento delle variabili casuali situate sopra quella determinata soglia (coda della distribuzione), EVT fornisce una sorta di Teorema del limite centrale (CLT) per le code di una distribuzione.

4.4.4 PRICING DEI RISCHI ESTREMI

I prodotti standard sono una sorta di swap che consentono a una controparte di assicurarsi contro un certo rischio di fronte al pagamento di un premio. Il prodotto più utilizzato nel rischio di credito è il Credit Default Swap (CDS), in cui una controparte riceve un premio per assicurare le perdite quando si viene colpiti dal rischio di credito[58] (Verlaine, 2020).
Una volta che il mercato esiste, il premio osservato può essere utilizzato per valutare i rischi attesi dal mercato, tuttavia un aspetto interessante riguarda i prodotti più complessi, che possono essere creati per estrarre delle informazioni sui molteplici tipi di rischio. In primo luogo, è possibile specificare diversi tipi di swap che tengono conto di tali tipi di rischi; lo sviluppo di prodotti di correlazione come tranche di primo livello e CDO[59] può essere impiegato per estrarre incertezza sul rischio di accumulo.

[58] Il premio dipenderà dalle perdite previste che vengono stimate valutando la probabilità di default e la loss given default
[59] Un obbligo di debito collateralizzato (CDO) è fondamentalmente un portafoglio di attività i cui rischi sono "venduti" a diverse controparti che copriranno diversi tipi di rischio.

Esistono diverse tranche con diversi gradi di rischiosità, dove la prima tranche copre i rischi iniziali a fronte del pagamento di un premio e le tranche senior sono meno rischiose e comportano un premio inferiore. Dato che, con l'accumulo del rischio, meno tranche rischiose vengono influenzate passo dopo passo, il premio implicito potrebbe essere utilizzato per estrarre le aspettative del mercato in merito al rischio di accumulo informatico e ricavare così la expected loss distribution.
Se si potessero creare prodotti con dimensioni di tranche abbastanza piccole, allora sarebbe possibile ricavare una distribuzione delle perdite sempre più precisa e isolare un qualche tipo di distribuzione di probabilità di perdita neutrale al rischio che, indicherebbe il prezzo Arrow-Debreu state per diversi livelli di perdita.
Se tale distribuzione venisse confrontata con approcci di modellazione più diretti come quelli sviluppati da Zhan *et* al. (2015) potrebbe fornire informazioni sul rischio neutro, rispetto a probabilità storiche. Tali informazioni possono essere utilizzate per valutare il peso delle informazioni per un decision maker che, ha accesso solo alle informazioni storiche e fornisce quelle sui prezzi impliciti di rischi informatici estremi.

4.5 IL MODELLO COPULA

Tramite le copule si cerca di sviluppare un modello di tariffazione della cyber assicurazione in cui i premi dipendono dal numero di computer interessati, dalla distribuzione delle perdite in euro a livello aziendale e dalla tempistica dell'evento di violazione. Herath S. e Herath T. (2011) con il loro lavoro, incorporano tre elementi di un contratto assicurativo standard: l'importo della liquidazione che viene pagato, il verificarsi dell'evento coperto dal contratto e il momento in cui la liquidazione viene pagata nel pricing della cyber insurance.
Il modello proposto applica la metodologia delle copule che, consente di acquisire dipendenze non lineari tra le variabili dei prezzi degli input, senza porre restrizioni al tipo di distribuzioni marginali considerate per le variabili di prezzo.
L'uso delle copule è essenziale, ma viene considerato relativamente nuovo per il settore dell'assicurazione informatica. Per la determinazione del pricing si illustra un modello di simulazione Monte Carlo basato appunto sulle copule e si utilizzano le distribuzioni di

perdite empiriche basate sui dati dell'indagine ICSA (2005) disponibili al pubblico[60].
I premi per le perdite relativi alla copertura di prima parte vengono calcolati utilizzando tre tipi di modelli di polizza assicurativa: polizze di base, polizze deducibili e polizze deducibili con coassicurazione.
Il termine copula fu coniato da Sklar (1959), ed è stato studiato per oltre quarant'anni; deriva dal latino copula = "unione", "legame" (da cum + apio = "attaccare") e fa riferimento a funzioni che uniscono o accoppiano quelle di distribuzione multivariata alle loro marginali unidimensionali; in alternativa, le copule possono essere descritte come distribuzioni multivariate i cui margini unidimensionali sono uniformi nell'intervallo [0, 1] (Frees e Valdez, 1998).
Esse riscuotono l'interesse degli statistici per due motivi principali: quali il modo di studiare le misure di dipendenza e come punto di partenza per la costruzione di famiglie di distribuzioni bivariate per la simulazione (Fisher, 1997).
Nel caso dell'assicurazione, ciò implica la modellizzazione delle dipendenze non lineari nelle variabili di prezzo e l'utilizzo della simulazione per determinare i premi.

4.5.1. VALUTAZIONE DEL CYBER RISK

Vi sono tre elementi di rischio che in genere fanno parte di qualsiasi contratto assicurativo (Klugman, 1986): l'ammontare della liquidazione che viene pagato; il verificarsi dell'evento coperto dal contratto e il momento in cui viene pagata la liquidazione.
Nel modello assicurativo proposto per la determinazione del prezzo di interruzione dell'attività di prima parte a causa di violazioni della sicurezza, la variabile casuale sconosciuta di interesse è l'importo (P) che, viene pagato dalla compagnia assicurativa. Esso dipenderà dall'importo della perdita in euro (Π), relativo ad un'impresa con (q) numero di computer/server interessati.
Supponiamo che π sia la perdita in euro osservata dai dati disponibili (ad esempio, dall'indagine sulla prevalenza del virus informatico dell'ICSA (2005)). Possiamo modellare la perdita (Π) relativa a un evento di violazione a livello di impresa in funzione di entrambi (q) e (π) dati da $\Pi = g(\pi, q)$. Nel modello ipotizziamo che la distribuzione

[60] In particolare, si utilizzano i dati a livello aziendale sul numero di computer interessati e sulle perdite in dollari dovute a incidenti di virus come punto di partenza per illustrare la valutazione della distribuzione empirica delle perdite congiunte che è essenziale per la determinazione del premio.

delle perdite per un l'impresa dipenda da due variabili casuali π e q. Dal momento che i dati affidabili su Π scarseggiano, le compagnie assicurative possono utilizzare i dati disponibili al pubblico come quelli dell'indagine ICSA (Bridwell, 2005) per modellare Π usando una copula appropriata.

Il tipo di dipendenza tra le variabili casuali; come (q) e (π), è cruciale sotto molti aspetti per la gestione del rischio informatico, perché esse sono intrecciate a causa della dipendenza parziale delle perdite e dal numero di computer colpiti da una violazione della sicurezza.

Il secondo elemento di rischio, il verificarsi dell'evento coperto dal contratto, è modellato da una variabile bernoulliana ω, che assume valore 1, se si verifica l'evento coperto o 0 in caso contrario.

Il terzo elemento di rischio è (T), ossia il tempo che intercorre tra l'emissione della polizza e il momento in cui la richiesta di risarcimento verrà liquidata[61]. Nella sicurezza delle informazioni, per eventi casuali, come le intrusioni di virus, la distribuzione di Poisson, è ampiamente utilizzata per modellare la comparsa delle intrusioni per unità di tempo. È possibile utilizzare il processo della velocità di intrusione di Poisson per determinare il tempo fino alla violazione del sistema IT. L'uso delle copule presuppone implicitamente che, gli eventi casuali che hanno causato le perdite siano reiterati.[62]

4.5.2 MODELLARE LA LOSS DISTRIBUTION MEDIANTE LE COPULE

La metodologia di Copula può essere utilizzata efficacemente per modellare la distribuzione congiunta delle perdite in euro a causa di attacchi informatici a livello aziendale (Herat S. e Herath T., 2011).

Una componente chiave dei prezzi assicurativi comprende e modella le relazioni multivariate; mentre la regressione lineare può fornire una base per spiegare la relazione tra due o più variabili. Il modello si basa su ipotesi di normalità e dipendenza lineare: la regressione lineare funzionerebbe se le distribuzioni marginali fossero normali, tuttavia la distribuzione marginale per il numero di computer interessati (q), e il valore in euro delle perdite (π), potrebbero non distribuirsi come una Normale. Nel caso della variabile

[61] È ragionevole supporre che il tempo tra l'incidente e la transazione sarà breve (o equivalentemente zero).
[62] Nel caso di danni di prima parte dovuti a virus, si può ragionevolmente supporre che l'evento di violazione casuale (intrusione di virus) seguirà probabilmente uno schema simile.

di prezzo e del numero di computer interessati (q), è probabile che la distribuzione marginale sia del tipo Pareto, Esponenziale o Weibull, poiché alcuni virus (15% -25%) rappresentano un gran numero di computer interessati (75%-85%).

Poiché le distribuzioni marginali non sono normali, la correlazione di Pearson (ρ), che misura un'eventuale relazione di linearità, non può essere utilizzata per modellare la dipendenza tra le due variabili, pertanto nel modellare la distribuzione delle perdite di un'azienda, l'uso delle copule è più appropriato.

Il primo passo si esprime nell'identificare la "copula appropriata" per modellare la dipendenza non lineare che spiega la relazione tra le due variabili di interesse , il numero di computer interessati (q) e il valore in dollari delle perdite (π). Sia l il limite inferiore e m quello superiore del numero di computer interessati. Supponendo che il valore in dollari delle probabili perdite possa essere ripartito in base al numero di computer interessati (o esposti) e che la seguente funzione acquisisca la specifica distribuzione delle perdite dell'azienda:

$$\Pi = g(\pi, q) = \begin{cases} a_1 & se\ q < l \\ a_2 + \left(\frac{q-l}{q}\right)\left(\frac{\pi}{10}\right) & se\ l \leq q < m \\ a_3 + \left(\frac{q-m}{q}\right)\left(\frac{\pi}{10}\right) & se\ q \geq m \end{cases} \tag{4.13}$$

dove

- a_i, i = 1, 2, 3 sono costanti.

I valori distribuiti congiuntamente per la distribuzione delle perdite di un'azienda Π=(g,π) possono essere calcolati usando la simulazione Monte Carlo.

Il modello probabilistico per il costo della cyber assicurazione per danni di prima parte, a causa di una violazione basata su elementi di rischio di un contratto di assicurazione è:

$$C = \omega e^{-rT} P\ ; \tag{4.14}$$

- ω è una variabile binaria, uguale a 1 se l'evento coperto si verifica e 0 altrimenti;
- T è il tempo fino all'incidente della violazione della sicurezza;
- r è il tasso di sconto;
- P è l'importo pagato dalla compagnia assicurativa in caso di violazione.

Per semplicità, si supponga che l'evento coperto si verifichi una sola volta durante il

periodo del contratto e che la perdita riguardi un singolo reclamo. Più specificamente, dato T momento della prima istanza di una violazione della sicurezza informatica, si ipotizzi che il sistema fallisca dopo la prima violazione e che il reclamo venga pagato una sola volta. Il premio netto è dato da:

$$E(C) = \bar{\omega}E(e^{-rT})E(P); \tag{4.15}$$

dove la probabilità che si verifichi un evento è $\bar{\omega} = E(\omega) = P(\omega = 1)$. Questo premio netto non include le spese e i profitti della compagnia assicurativa; per ottenere il premio effettivo addebitato è necessario aggiungere un determinato importo a copertura delle spese e i profitti.

1. Polizza di primo tipo: polizza di base per danni di prima parte con franchigia zero. Supponiamo di considerare una cyber policy che abbia una franchigia (d)[63], un importo di perdita (Π) e (P) l'importo pagato, quindi le relazioni tra polizze sono modellate come:

$$P = \Pi = g(\pi, q) \tag{4.16}$$

2. Polizza di secondo tipo: polizza per danni di prima parte con franchigia.

$$P = \begin{cases} 0 & se\ \Pi \leq d \\ \Pi - d & se\ \Pi > d \end{cases} \tag{4.17}$$

3. Polizza di terzo tipo: polizza per danni di prima parte con coassicurazione e limite: si considera un terzo modello con una franchigia *d*, la coassicurazione di *a* e un limite di *k*. L'assicurazione non paga nulla quando la perdita è inferiore a *d*, paga il 100% *(1 - a)* delle perdite in eccesso rispetto a *d*, ma non paga mai nulla in eccesso. La relazione tra la variabile casuale di interesse P e la variabile casuale osservata Π può essere modellata come:

$$P = \begin{cases} 0, & se\ \Pi \leq d \\ (1-a)(\Pi - d), & se\ d < \Pi < d + \frac{k}{1-a} \\ k\ , & se\ \ \Pi > d + \frac{k}{1-a} \end{cases} \tag{4.18}$$

[63] Variabile casuale osservata.

la variabile osservata è nota (può essere per esempio stimata dai dati ICSA (2005)), ma non si dispone di dati storici sugli importi effettivi pagati (P) dalle compagnie assicurative né il numero di polizze per stimare la frequenza di $\bar{\omega}$. Quindi, essendo a conoscenza di Π, possiamo supporre che quando Π > 0 (si sia verificata una perdita), in tal caso si è realizzato l'evento e quindi $\omega = 1$. Tuttavia, poiché non si dispone dei dati per stimare la frequenza e l'obiettivo principale è quello di illustrare l'approccio delle copule nel contesto di sicurezza IT, si assume che $\bar{\omega} = 1$.

L'altra variabile sconosciuta è T, il tempo dal momento in cui la polizza viene emessa fino al pagamento della liquidazione, che può essere modellata utilizzando una Poisson. In una distribuzione di Poisson con un tasso di arrivo previsto di λ intrusioni per unità di tempo, il numero di eventi che si verificano in qualsiasi periodo di tempo t è λ_t[64] . Pertanto, i tempi tra le intrusioni successive $A_i = t_1 - t_{(i-1)}$ sono variabili casuali esponenziali indipendenti con media $\frac{1}{\lambda}$.

Ipotizzando che $t_{(i-1)}$ sia stato determinato, per generare il prossimo tempo di arrivo t_i, la procedura è la seguente:

1. Generare una variabile casuale uniforme $u \sim \cup(0,1)$ indipendente;
2. restituire $t_i = t_{(i-1)} - \ln u \left(\frac{1}{\lambda}\right)$[65]

Quindi, dopo aver generato una variabile uniforme compresa tra 0 e 1, si calcola tramite il secondo passo della procedura, l'istante di comparsa della successiva violazione dato il tempo di manifestazione della precedente e il parametro λ della distribuzione di Poisson che descrive il numero previsto di intrusioni per unità di tempo (12 mesi).

4.5.3 PRICING DELLA CYBER INSURANCE

Nell'algoritmo integrato di simulazione basato sulle copule per la determinazione del pricing di una cyber policy di danni di prima parte, a causa di una violazione della sicurezza IT, sono previsti 5 passaggi (Herat S. e Herath T., 2011):

1. adattare una copula ai dati empirici (q, π). Successivamente, generare una sequenza di dati bivariati (q_k, π_k) per la k-esima iterazione usando la copula inserita (ad es. Clayton o Gumbel o qualsiasi altra copula).

[64] Da notare che il numero di eventi che si verificano in periodi separati sono indipendenti l'uno dall'altro.
[65] Da specificare che $t_0 = 0$

2. Per ciascuna sequenza di dati bivariati (q_k, π_k) nel passaggio precedente, calcolare le perdite Π^k= g (q_k, π_k) usando l'equazione 4.13.
3. Si modella la prima richiesta di una violazione della sicurezza o il tempo fino all'incidente usando la procedura di simulazione di Poisson $T^k = t_1^k = t^k - ln\, u^k \left(\frac{1}{\lambda}\right)$
4. Calcolare il premio assicurativo per k-esima iterazione come $C^k = \omega P^k e^{-\delta T^k}$
5. Calcolare il valore atteso e la deviazione standard del premio assicurativo come:

$$E[C] = \frac{1}{S} \sum_{k=1}^{S} C^k = \frac{1}{S} \sum_{k=1}^{S} \omega P^k e^{-\delta T^k} \qquad (4.19)$$

$$\sigma[C] = \sqrt{\frac{\frac{1}{S}\sum_{k}^{S}\left(C^k\right)^2 - [E(C)]^2}{S}} \qquad (4.20)$$

4.5.4 CONSIDERAZIONI SULL'APPROCCIO

La letteratura sulla cyber-assicurazione non ha mai preso esplicitamente in considerazione questi aspetti dell'assicurazione che, sono fondamentali per modellare in modo appropriato i rischi associati a un contratto di cyber insurance: il verificarsi dell'evento[66], il momento in cui viene pagata l'assicurazione e l'importo pagato (Herat S. e Herath T., 2011).

Un altro aspetto importante è l'utilizzo di dati esistenti, in particolare dei dati dell'indagine ICSA (2005) disponibili al pubblico, per lo sviluppo e l'illustrazione del pricing della cyber assicurazione. Un punto importante indicato dai dati è che le distribuzioni marginali potrebbero non essere normali: la dipendenza tra il numero di computer interessati e le perdite (calcolate in euro o dollaro) è correlata, ma non nel tipico modo lineare, quindi la solita misura di dipendenza, che è la correlazione di Pearson, non è utilizzabile. Questo problema è significativo in quanto le perdite tendono ad essere distribuite in modo pareto con pochi virus o pochi incidenti di hacking con conseguenti perdite ingenti e che colpiscono un gran numero di computer.

Al fine di valutare adeguatamente il rischio a livello di impresa, si illustra l'approccio

[66] Con evento si intende la violazione coperta dalla cyber policy.

delle copule per la modellizzazione della dipendenza dei rischi; questa è una tecnica più solida per ottenere le distribuzioni congiunte delle perdite per due motivi: innanzitutto permette di tenere presenti le dipendenze non lineari per i rischi correlati, in secondo luogo, è un approccio versatile, poiché consente di simulare da un modello di copula senza dover esplicitamente determinare la distribuzione congiunta per i due dati marginali.

4.5.5 LIMITI E OSTACOLI PER FUTURE RICERCHE

Uno dei principali vincoli nel pricing della cyber insurance, è la scarsità di dati sui cyber crimini e le relative perdite (Baer e Parkinson, 2007), problema ulteriormente acuito dal fatto che le aziende non rivelano dettagli relativi a violazioni della sicurezza (Gordon et al., 2003).

La scarsità di dati è una limitazione dell'approccio della copula proposto, poiché esso utilizza i dati per determinare la copula appropriata e valutare i premi annuali netti medi. Un'altra limitazione è la qualità dei dati: è più probabile che π dipenda dal numero di vulnerabilità, che può dipendere dalle precauzioni di sicurezza adottate dall'azienda[67]. In caso di incidente, le perdite dipenderanno dal tipo di computer interessato e dall'utente; le violazioni della sicurezza spesso comportano numerosi tipi di perdite: la perdita di produttività, le potenziali entrate, i costi di pulizia e l'impatto sulla performance finanziaria,....

Vi è un ampio spazio per la ricerca futura, compresi gli argomenti come lo sviluppo di polizze informatiche basate sulla diversità dei prodotti (hacking, malware, ecc.), posture di sicurezza, l'integrazione di ulteriori rischi correlati, ecc. Una lenta crescita nel settore delle assicurazioni informatiche può essere parzialmente attribuita al fatto che, le perdite derivanti da violazioni della sicurezza sono fortemente correlate a causa di Internet. Il problema dell'alta correlazione tra gli assicurati nella cyber insurance è contrario al principio del bilanciamento del portafoglio in altri tipi di servizi assicurativi. Questo problema, tuttavia, è endogeno e non può essere evitato poiché Internet è un mezzo condiviso a livello globale.

[67] Ad esempio, il monitoraggio e l'aggiornamento quotidiani dei virus è meno rischioso rispetto al monitoraggio e aggiornamento settimanale.

4.5.6 CONCLUSIONI

L'approccio discusso aumenta la consapevolezza sull'importanza di raccogliere dati relativi alle violazioni della sicurezza per la negoziazione di premi più bassi sui prodotti di cyber assicurativi. Molti ricercatori in materia di sicurezza IT sottolineano il fatto che, uno dei principali problemi per l'industria della cyber insurance è la disparità di premi e la mancanza di modelli quantitativi innovativi.

La maggior parte dei prodotti assicurativi tradizionali utilizza dati raccolti storicamente per determinare i premi assicurativi, allo stesso modo, le compagnie assicurative possono raccogliere nel tempo i dati relativi al rischio informatico e successivamente modificare i modelli. È ragionevole ipotizzare se la cyber insurance sarà utile o dannosa nell'ambito di sicurezza IT, a causa della problematica legata al rischio morale (Gordon et al., 2003), tuttavia combinata con adeguati investimenti in sicurezza IT, essa consente alle aziende di gestire meglio i cyber risk.

Nonostante i limiti, questo approccio basato sulle copule fornisce un significativo contributo metodologico nell'area della sicurezza informatica, in quanto fornisce una prospettiva di modellazione teoricamente solida, utilizzando un approccio attuariale per valutare i premi assicurativi per i prodotti di cyber insurance. Questo appare il primo metodo nella letteratura sulla sicurezza delle informazioni a integrare elementi standard di rischio assicurativo con la solida metodologia delle copule.

Capitolo 5

5. PRESENTAZIONE DEI PROCESSI EPIDEMICI E SIMULAZIONE DEL PRICING TRAMITE IL METODO COPULA

5.1. I PROCESSI INFETTIVI O EPIDEMICI

I modelli epidemici sono stati ampiamente utilizzati al fine di analizzare le interazioni nelle reti, ad esempio, attacco e propagazione di virus nelle reti di computer, voci che girano nei social network e guasti a cascata (Bichara et al., 2013). L'evoluzione dell'epidemia nella rete può essere associata allo studio della propagazione di malattie infettive, cosicché si tiene conto dei possibili stati di un ospite rispetto alla malattia:

- suscettibile (S). Questi sono gli individui (nel nostro caso computer e/o server) suscettibili di contrarre la malattia se sono esposti ad essa;
- esposto (E). Questi individui (computer e/o server) hanno contratto la malattia ma non sono ancora infetti, quindi non ancora in grado di trasmettere la malattia al gruppo S;
- infetto (I). Dopo essere stati esposti, questi individui sono ora in grado di trasmettere la malattia ad altri individui nel gruppo S;
- recuperato (R). Dopo aver attraversato le fasi precedenti della malattia, gli individui guariscono perché hanno sviluppato un'immunità da essa (permanente o temporanea).

Non tutti i modelli epidemiologici includeranno tutte e quattro le classi e alcuni con un maggiore grado di sofisticazione potrebbero includerne di più (Allen, 1994). Sulla base della selezione o dell'omissione di queste classi, che di per sé implica alcuni presupposti in base alle caratteristiche della malattia specifica che si cerca di modellare, ci sono diversi acronimi utilizzati per nominare questi modelli. Ad esempio, in un modello SI, noto anche come semplice modello epidemico, l'ospite non recupera mai. Un modello SIS è quello in cui la popolazione suscettibile viene infettata e quindi, dopo essersi ripresa dalla malattia e dai suoi sintomi, diventa nuovamente suscettibile. Il SIR (suscettibili,

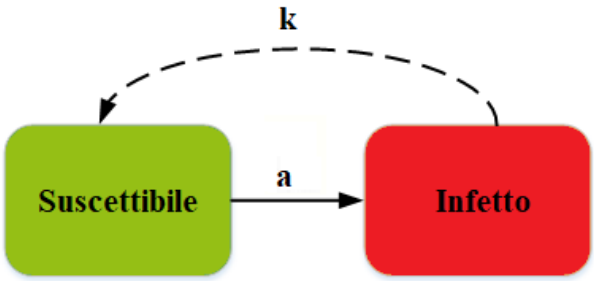
infetti e rimossi) è invece un modello in cui gli individui sensibili vengono prima esposti (ma non ancora infetti), poi entrano nel gruppo degli infetti, diventando veicolo dell'infezione e infine entrano nel gruppo R quando cessano di diventare infetti e sviluppano l'immunità.

5.1.1. IL MODELLO SIS

I modelli SIS di epidemie comprendono due classi: S e I. Nel nostro caso è lecito supporre che (Bichara et al., 2013):

- la popolazione è finita, quindi N rimane costante in ogni momento;
- gli individui (nel nostro caso i computer e/o server) passano dall'essere sensibili alla malattia (riferita al malware) e successivamente all'essere infetti e di nuovo all'essere sensibili in seguito alla guarigione;
- la malattia (malware) è tale da non permettere lo sviluppo di un'immunità permanente o temporanea e non vi sono mortalità;
- il numero di infezioni di individui sensibili (computer e/o server) che si verificano è proporzionale al numero di contatti tra individui (computer e/o server) infetti e sensibili;
- ad ogni unità di tempo, una certa percentuale k di individui (computer e/o server) infetti che guarisce dalla malattia e diventa di nuovo suscettibile. Ciò equivale a dichiarare che la durata media del periodo di infezione sia $\frac{1}{k}$ unità di tempo.

Figura 5.1: Epidemia cibernetica descritta dal tasso α che rappresenta il tasso di infezione e k che esprime il tasso di recupero.



Fonte: *SIS* and *SIR* epidemic models under virtual dispersal (Bichara et al., 2015).

Il parametro k rappresenta quindi la percentuale di individui infetti che si riprendono ad ogni unità di tempo e diventano di nuovo sensibili, il parametro α rappresenta la percentuale di contatti che causano un'infezione e γ è il tasso di contatto tra persone (computer e/o server) infette e sensibili.

In linea di principio si dovrebbe cercare di avere il minor numero possibile di parametri in un modello, tanto più in questo caso, poiché i due parametri possono essere considerati come uno: $\beta = \frac{\alpha}{\gamma}$, utilizzato per rappresentare la percentuale di casi dalle popolazioni suscettibili e infette complessive che causano effettivamente un'infezione.

Quindi il modello risultante è:

$$\frac{dS}{dt} = -\beta SI + kI \tag{5.1}$$

$$\frac{dI}{dt} = \beta SI - kI \tag{5.2}$$

Dal momento che N è il totale della popolazione (computer e/o server) composta dalla somma degli S e I, quindi N=S+I, e ponendo I=N-S, in equilibrio abbiamo:

$$\beta S^2 - S(k + \beta N) + kN = 0 \tag{5.3}$$

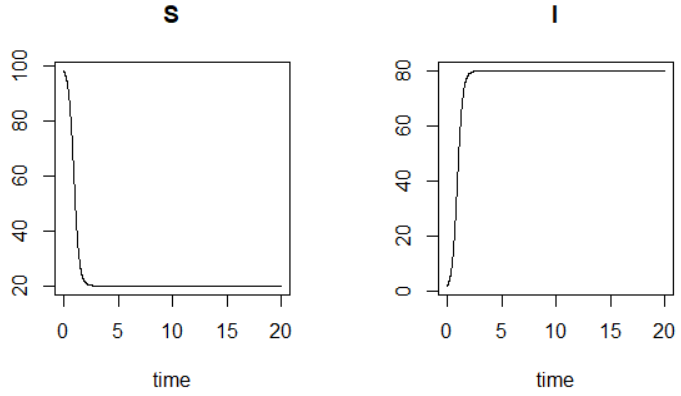
A livello intuitivo, possiamo notare che in un istante temporale, gli individui sensibili stanno diventando infetti, ma qualche istante dopo, gli stessi individui infetti stanno diventando nuovamente sensibili. C'è un meccanismo di feedback negativo in atto qui, perché ogni classe si basa su una maggiore quantità di individui che si trovano nella classe opposta per crescere in numero. In altre parole, la mancanza di individui suscettibili assicura che, la popolazione di individui infetti inizierà a diminuire, il che può significare solo che ci saranno individui più sensibili in futuro, poiché la popolazione complessiva rimane costante. E precisamente cos'è questo equilibrio? Possiamo aspettarci che la malattia alla fine si estinguerà da sola o al contrario, tutti saranno infettati? In uno stato di equilibrio, le variabili di stato non cambiano, quindi una qualsiasi delle derivate sopra può essere impostata su 0 (Bichara et al., 2015).

L'equazione 5.1 è una semplice equazione quadratica le cui radici sono S = $\frac{k}{\beta}$ e S = N questi sono gli stati di equilibrio per il numero di individui sensibili. Se lo stato di equilibrio per la popolazione sensibile S è uguale a N, alla fine tutti diventeranno sensibili e nessuno sarà infettato, quindi la malattia si estinguerà; se al contrario nessuno guarisce dall'infezione k = 0, alla fine tutti saranno infettati e non ci saranno soggetti sensibili.

Il seguente modello di simulazione R, eseguito per tre diverse combinazioni dei parametri k e β[68], serve a convalidare la semplice analisi matematica derivante dall'equazione 5.3. Ogni simulazione inizia con I = 2 computer infetti e S = 98 suscettibili, ma indipendentemente dai valori iniziali, è possibile notare che la popolazione sensibile allo stato stazionario raggiunge $\frac{k}{\beta}$ o N.

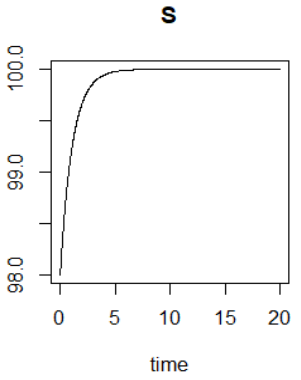
```
library(simecol)
N <- 100  #popolazione totale
sis <- odeModel(main=function(t, y, parms)
{
p <- parms
dS <- p["k"]*y["I"]-p["b"]*y["S"]*y["I"]  #equazione 5.1
dI <- -p["k"]*y["I"]+p["b"]*y["S"]*y["I"]  #equazione 5.2
list(c(dS, dI)) },
times=c(from=0,to=20,by=0.01),
init=c(S=N-2,I=2),  #imposto i valori iniziali
parms=c(k=1,b=0.05), #imposto il valore del tasso k e del tasso β
solver="lsoda")
simsis <- sim(sis)
plot(simsis)
```

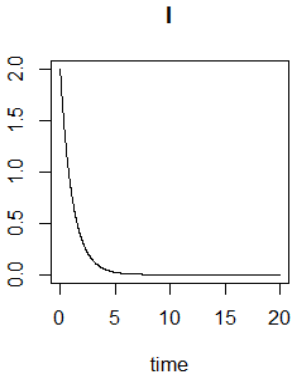
Figura 5.2: Output R della simulazione del modello epidemico SIS avente diversi tassi di infezione k e β



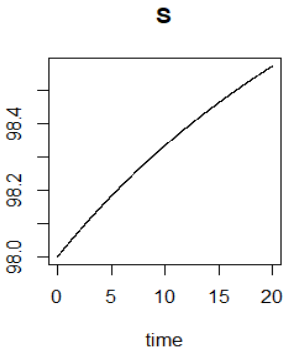
k=1 e $\beta = 0{,}05$
In questa prima simulazione notiamo che il numero di computer suscettibili cade a picco, reazione opposta per i soggetti infetti.

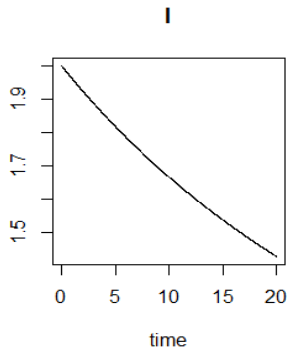
[68] Ricordando che k rappresenta la percentuale di computer infetti che "guarisce" dalla "malattia", mentre β indica la percentuale di computer sani che viene colpito dal malware.





k=1 e $\beta = 0{,}001$
Andando ad abbassare il valore del secondo parametro notiamo che il numero di computer suscettibili sale vertiginosamente, reazione opposta per i soggetti infetti.





k=1 e $\beta = 0{,}01$
Andando a immettere tale valore nel secondo parametro notiamo che il numero di computer suscettibili sale lentamente fino a che S equivale ad N, reazione uguale e contraria per i soggetti infetti che scendono fino a 0

5.1.2. IL MODELLO SIR

Il modello di malattia SIR fu proposto per la prima volta nel 1927 da Kermack e McKendrick, da cui la denominazione alternativa del modello epidemico di Kermack-McKendrick (Li e Zou, 2009). Con questo modello, i ricercatori hanno cercato dare risposte sul perché le malattie infettive si propagano improvvisamente e poi si spengono senza lasciare tutti infetti. Si parte dal presupposto che la popolazione è composta da tre tipi di individui, indicati dalle lettere S, I e R dove:

- S è il numero di soggetti sensibili, che non sono infetti ma potrebbero infettarsi;
- I è il numero di infetti, cioè individui che hanno la malattia e possono trasmetterla ai soggetti suscettibili;
- R è il numero di individui recuperati, cioè quei tipi di soggetti che possono o meno avere la malattia, ma non possono infettarsi e non possono trasmettere la malattia ad altri. Possono avere un'immunità naturale o potrebbero essersi ripresi dalla malattia e sono immuni dal riprenderla, oppure potrebbero avere la malattia, ma

non sono in grado di trasmetterla (ad es. perché potrebbero essere stati messi in isolamento oppure morti).

Il modello che prenderò in considerazione presuppone una scala temporale breve non considerando nascite e morti.[69] Quando si verifica una nuova infezione, l'individuo infetto si sposta dalla classe sensibile alla classe infettiva, non c'è altro modo in cui gli individui possono entrare o uscire dalla classe sensibile, quindi prima equazione differenziale è data da:

$$\frac{dS}{dt} = -\beta IS + \xi R \tag{5.4}$$

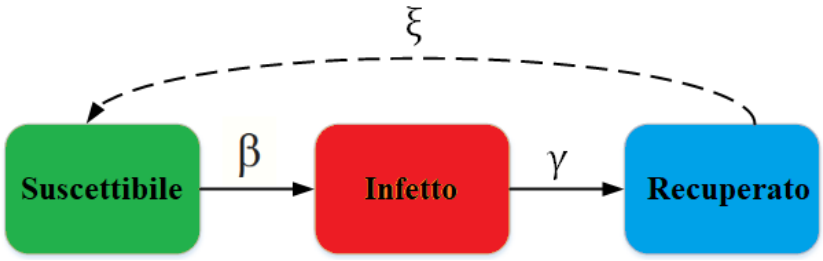
L'altro evento che può verificarsi è che gli individui infetti entrino nella classe dei recuperati, dato da:

$$\frac{dR}{dt} = \gamma I - \xi R \tag{5.5}$$

Quindi, per differenza, dal momento che il totale della popolazione viene posto uguale a 1 e calcolato come N = S + I + R, allora:

$$\frac{dI}{dt} = \beta IS - \gamma I \tag{5.6}$$

Figura 5.3: Epidemia cibernetica descritta dal tasso β che rappresenta il tasso di infezione, γ esprime il tasso di recupero e ξ descrive la velocità con cui un individuo recuperato ritorna suscettibile, perdendo così l'immunità.



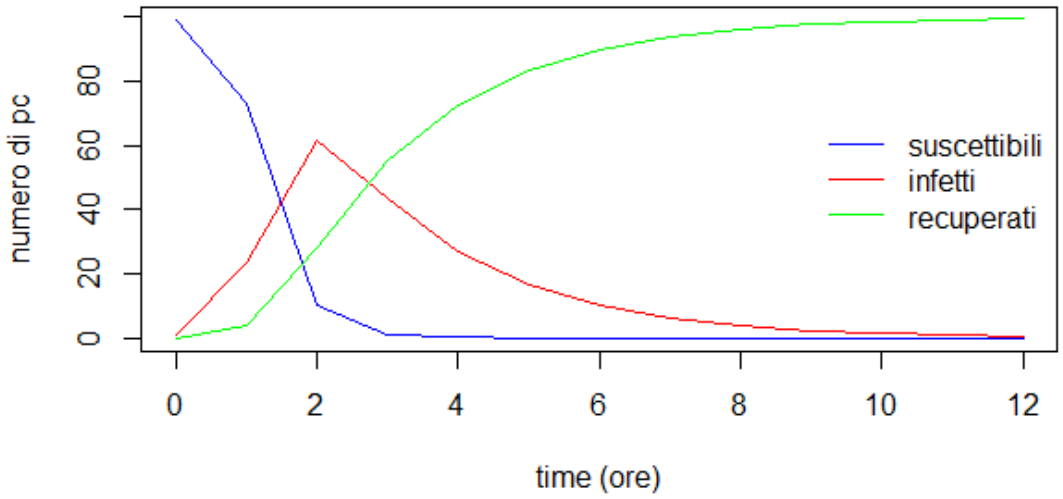
Fonte: Generalization of the Kermack-McKendrick SIR Model to a Patchy Environment for a Disease with Latency (Li e Zou, 2009).

[69] Il modello è basato su una popolazione formata da computer e/o server e l'infezione è data da un cyber virus o malware per questo non vengono prese in considerazione nascite o morti nell'arco temporale considerato.

Ho eseguito un modello di simulazione R con parametri $\gamma = 0.5$ (tasso di recupero per unità oraria) e $\beta = 0.04$ (tasso di infezione del virus). La simulazione inizia con I = 1 computer infetto, S = 99 suscettibili e R=0 computer recuperati.

```
library(deSolve)
equazione_sir <- function(time, variables, parameters) {
with(as.list(c(variables, parameters)), {
dS <- -beta * I * S    # equazione 5.4
dI <-  beta * I * S - gamma * I   # equazione 5.5
dR <-  gamma * I   # equazione 5.6
return(list(c(dS, dI, dR))) }) }
parametri <- c(
  beta  = 0.04, # tasso di infezione del virus (computer/ora)
  gamma = 0.5 )    # tasso di recupero (ogni ora)
valori_iniziali <- c(
  S = 99,  # suscettibili al tempo 0
  I =   1,  # infetti al tempo 0
  R =   0 )   # recuperati al tempo 0
time_values <- seq(0, 12) # ore
valori_sir_1 <- ode(
y = valori_iniziali, times = time_values, func = equazione_sir, parms = parametri )
valori_sir_1 <- as.data.frame(valori_sir_1)
with(valori_sir_1,
{
# metto a grafico la time series dei pc suscettibili, infetti e recuperati
 plot(time, S, type = "l", col = "blue", xlab = "time (ore)", ylab = "numero di pc")
lines(time, I, col = "red") lines(time, R, col = "green") })
# aggiungo la leggenda
legend("right", c("suscettibili", "infetti", "recuperati"),
col = c("blue", "red", "green"), lty = 1, bty = "n")
```

Figura 5.4: Grafico che descrive l'andamento degli individui suscettibili S (linea blu), degli individui infetti I (linea rossa) e degli individui recuperati R (linea verde) nell'arco di 12 ore.



Ponendo $\boldsymbol{\beta}$**=0.04 e** γ=0.5 notiamo dal grafico che gli individui suscettibili diminuiscono fino a raggiungere lo 0 dopo 3 ore invece i computer infetti salgono fino a colpire il picco in corrispondenza di 60 dopo 2 ore, per poi scendere lentamente ma costantemente nell'arco delle successive 10 ore; la curva dei computer recuperati sale molto velocemente fino a toccare l'apice intorno all'ottava ora. Per comodità e logica, il tasso ξ, cioè il tasso che descrive la velocità di ritorno alla suscettibilità da parte dei computer recuperati è stato posto uguale a 0, ciò significa che un computer recuperato diventerà immune all'infezione.

5.2 LE FUNZIONI COPULA

L'interesse per le copule nasce da diverse prospettive: in primo luogo, gli econometrici spesso possiedono una maggior quantità di informazioni sulle distribuzioni marginali delle variabili correlate, rispetto alla loro distribuzione congiunta[70], in secondo luogo, in un contesto bivariato, le copule possono essere utilizzate per definire misure non

[70] L'approccio della copula è un metodo utile per derivare distribuzioni congiunte date le distribuzioni marginali, specialmente quando le variabili non sono normali.

parametriche di dipendenza per coppie di variabili casuali[71], infine esse sono utili estensioni e generalizzazioni di approcci per la modellizzazione di distribuzioni e dipendenze congiunte apparse in letteratura (Herath e Herath, 2011).
Secondo Schweizer (1991), il teorema alla base delle copula fu introdotto in un articolo del 1959 di Sklar, scritto in francese, a cui fece seguito un articolo simile, scritto in inglese nel 1973 dallo stesso autore.

Teorema 5.1 (Sklar, 1973) Date le funzioni di distribuzione marginale $F_1(y_1), \dots, F_m(y_m)$, allora $\forall y = (y_1, \dots, y_m) \in R^n$ e una funzione cumulativa di distribuzione, CDF, d-dimensionale.

i. Se C è una copula il cui dominio contiene $Ran(F_1)\ x \dots x\ Ran(F_d)$, dove Ran($F_i$) denota il rango di CDF, allora $C\big(F_1(y_1), \dots, F_m(y_m)\big)$ è una funzione di distribuzione congiunta con marginali $F_1(y_1), \dots, F_m(y_m)$.
ii. Al contrario, se H è una funzione di distribuzione congiunta con marginali $F_1(y_1), \dots, F_m(y_m)$, allora esiste una copula C, con dominio $Ran(F_1)\ x \dots x\ Ran(F_d)$ tale che $H(y) = C\big(F_1(y_1), \dots, F_m(y_m)\big)$

Se $F_1(y_1), \dots, F_m(y_m)$, sono continue, la copula è unica, altrimenti essa è unicamente determinata in $Ran(F_1)\ x \dots x\ Ran(F_d)$.
In poche parole le copula sono funzioni che collegano le distribuzioni multivariate ai loro margini unidimensionali. Se F è una funzione di distribuzione cumulativa m-dimensionale (cdf [72]) con margini unidimensionali $F_{1,\dots}, F_m$, allora esiste una copula m-dimensionale C tale che:

$$F(y_1, \dots, y_m) = C\big(F_1(y_1), \dots, F_m(y_m)\big)^{73} \tag{5.7}$$

Il termine copula fu introdotto da Sklar (1959), tuttavia, l'idea apparve già in precedenza in numerosi testi: Hoeffding nel 1940 in particolare stabilì i migliori limiti possibili per queste funzioni e studiò le misure di dipendenza su trasformazioni in costante aumento (Schweizer, 1991).

[71] Quando sono rilevanti modalità di dipendenza abbastanza generali e/o asimmetriche come quelle che vanno oltre la correlazione o l'associazione lineare, le copula svolgono un ruolo speciale nello sviluppo di ulteriori concetti e misure.
[72] Cumulative distribution function.
[73] Il caso m = 2 ha attirato molta attenzione.

Le copule si sono rivelate utili in una varietà di situazioni di modellazione:

- gli istituti finanziari si preoccupano spesso se i prezzi di diverse attività presentino dipendenza, in particolare nelle code delle distribuzioni congiunte. Questi modelli presuppongono in genere che i prezzi delle attività abbiano una distribuzione normale multivariata, ma Ane e Kharoubi (2003) ed Embrechts et al. (2003) sostengono che questa ipotesi è spesso insoddisfacente, perché si osservano più frequentemente grandi cambiamenti rispetto a quanto previsto dall'assunzione della normalità. Il valore al rischio (VaR) stimato secondo la normale multivariata può portare a una sottovalutazione del VaR di portafoglio. Poiché le deviazioni dalla normalità, ad esempio la dipendenza dalla coda nella distribuzione dei prezzi delle attività, aumentano notevolmente le difficoltà computazionali dei modelli di attività comuni, la modellazione basata su una copula parametrizzata da marginali non normali è un'alternativa interessante .
- Gli attuari sono interessati ai modelli di valutazione delle rendite in cui la relazione tra l'incidenza di due individui sulla malattia o sulla morte è correlata congiuntamente (Clayton, 1978). Ad esempio, gli attuari hanno notato l'esistenza di una sindrome del "cuore spezzato" in cui la morte di un individuo aumenta sostanzialmente la probabilità che, anche il coniuge della persona subisca la morte entro un determinato periodo di tempo. Il coniuge sopravvissuto infatti tende ad esibire un comportamento non lineare con forte dipendenza dalla coda, quindi scarsamente adatto a modelli basati sulla normalità, di conseguenza candidandosi per la modellazione sulla base delle copula.
- Molte situazioni di modellizzazione microeconometrica hanno distribuzioni marginali che, non possono essere facilmente combinate in distribuzioni congiunte; ciò si presenta spesso nei modelli di variabili discrete o dipendenti limitate[74]; inoltre, la modellizzazione congiunta è particolarmente difficile quando due variabili correlate provengono da diverse famiglie parametriche, ad esempio, una variabile potrebbe caratterizzare una scelta discreta multinomiale e un'altra potrebbe misurare un conteggio degli eventi. Dato che, esistono poche o nessuna distribuzione parametrica congiunte basate su marginali di famiglie diverse, l'approccio copula fornisce quello generale e diretto per la loro costruzione.

[74]Le distribuzioni bivariate di conteggi di eventi discreti sono spesso restrittive e difficili da stimare.

- In alcune applicazioni, una distribuzione congiunta flessibile fa parte di un problema di modellazione più ampio, ad esempio, nel modello di auto-selezione lineare, una variabile di successo come il reddito viene osservata solo se si verifica un altro evento (ad esempio la partecipazione della forza lavoro). La distribuzione di probabilità per questo modello include una distribuzione congiunta per la variabile reddito e la probabilità che l'evento venga osservato. Di solito, si presume che questa distribuzione sia normale multivariata, ma Smith (2011) dimostra che per alcune applicazioni una rappresentazione flessibile delle copule è più appropriata.

5.2.1 Il FUNZIONAMENTO DELLE COPULE

Usando R genero n campioni da una distribuzione normale multivariata di 3 variabili casuali data la matrice di covarianza sigma usando il pacchetto MASS (Yan, 2007).

```
library(MASS)
> set.seed(100)
> m <- 3
> n <- 1000
> sigma <- matrix(c(1, 0.3, 0.15,
+                   0.15, 1, -0.6,
+                    0.3, -0.6, 1),
+        nrow=3)
> z <- mvrnorm(n,mu=rep(0, m),Sigma=sigma,empirical=T)
```

Successivamente controllo la correlazione dei campioni usando cor () e un grafico di correlazione a coppie impostando method = 'spearman' per utilizzare il rho di Spearman[75] invece del metodo 'pearson' nella funzione cor ().

```
> library(psych)
```

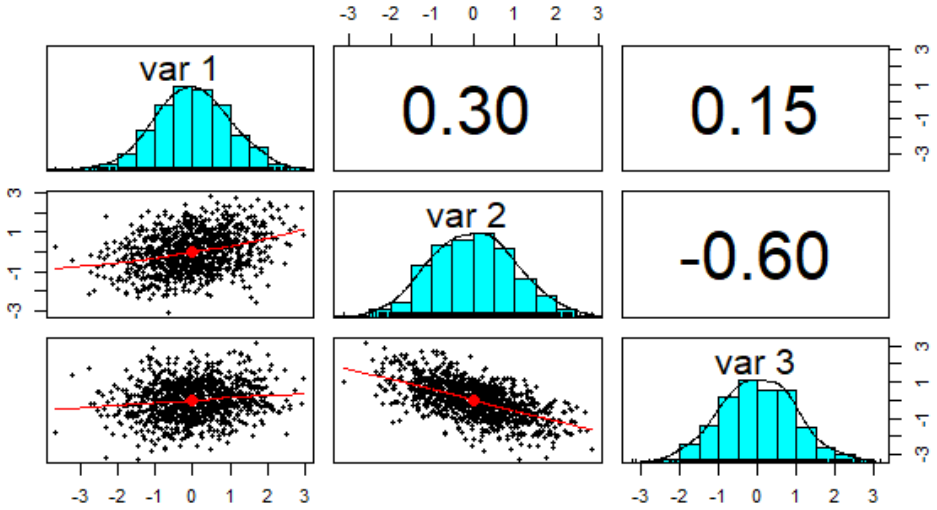
[75] L'indice di correlazione di Spearman, o Rho di Spearman, permette di valutare la forza della relazione tra due variabili quando il coefficiente di correlazione di Pearson non è soddisfatto. In particolare, quando la distribuzione delle variabili X e Y non risulta normale, o quando le sottopopolazioni dei valori di Y o X non presentano la stessa varianza, non si utilizzerà la correlazione parametrica ma si ricorrerà invece a questo indice che ha inoltre modalità di calcolo piuttosto semplice.

```
cor(z,method='spearman')
```

```
           [,1]       [,2]       [,3]
[1,] 1.0000000  0.2829835  0.1430740
[2,] 0.2829835  1.0000000 -0.5928814
[3,] 0.1430740 -0.5928814  1.0000000
```

```
> pairs.panels(z)
```

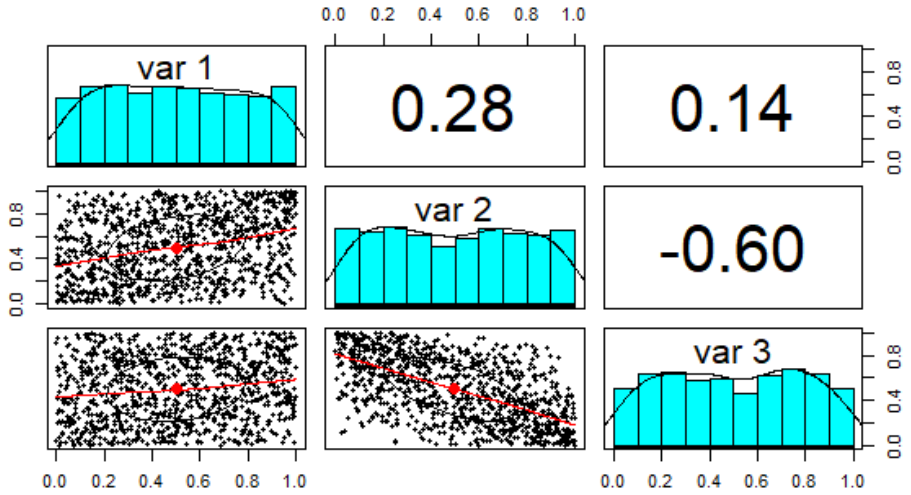
Figura 5.5: Grafico che descrive la correlazione a coppie tra le tre variabili; nella diagonale principale si notano le tre varianze.



Se X è una variabile casuale con distribuzione F, allora F(X) si distribuisce uniformeme nte nell'intervallo [0, 1].

```
> u <- pnorm(z)
> pairs.panels(u)
```

Figura 5.6: Grafico che descrive la correlazione a coppie tra le tre variabili adattate alla distribuzione uniforme $U \sim (0, 1)$.



La figura precedente rappresenta il diagramma delle nostre nuove variabili casuali contenute in u. Si noti che, ogni distribuzione è uniforme nell'intervallo [0,1], inoltre la correlazione è la stessa, infatti, la trasformazione applicata non ha modificato la correlazione tra le variabili casuali, quello che rimane è la struttura di dipendenza.
Come ultimo passo, si andranno a selezionare le marginali, che verranno poi applicate all'uniforme. Ho scelto come distribuzioni marginali la Gamma, Beta e infine la t-Student distribuite con i parametri specificati di seguito.

```
> x1 <- qgamma(u[,1],shape=2,scale=1)
> x2 <- qbeta(u[,2],2,2)
> x3 <- qt(u[,3],df=5)
```

Dopodiché è fondamentale notare che, partendo da un campione normale multivariato si andrà a creare un campione con la struttura di dipendenza desiderata a partire da distribuzioni marginali scelte in modo arbitrario.

```
df <- cbind(x1,x2,x3)
```

Viene utilizzato il comando cbind per combinare per colonna e riga le tre distribuzioni marginali
In seguito, esamino la correlazione usando sempre il metodo di Spearman.

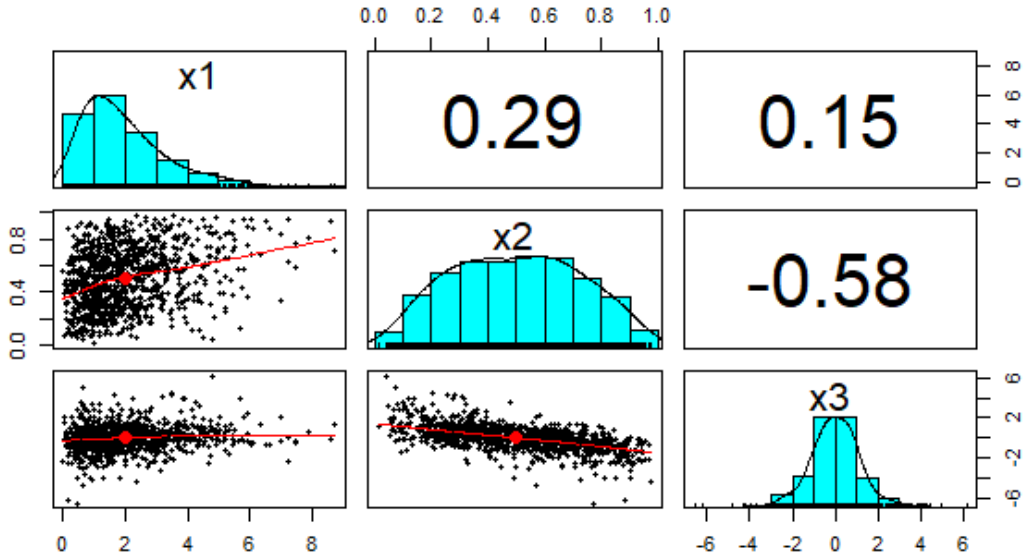
```
> cor(df,meth='spearman')
```

```
           x1         x2         x3
x1 1.0000000  0.2829835  0.1430740
x2 0.2829835  1.0000000 -0.5928814
x3 0.1430740 -0.5928814  1.0000000
```

```
> pairs.panels(df)
```

Il grafico che segue rappresenta le correlazioni a coppie.

Figura 5.7: Grafico che descrive la correlazione a coppie tra le tre differenti distribuzioni marginali (Gamma, Beta e t-Student).



L'intera simulazione appena eseguita può essere risolta in maniera più efficiente, concisa e curata mediante l'uso del pacchetto copula, quindi si cerca di replicare il processo usando le copula.

```
> library(copula)
> set.seed(100)
> nCop <- normalCopula(param=c(0.3,0.15,-0.6), dim = 3, dispstr = "un")
> mvdcop <- mvdc(copula=nCop, margins=c("gamma", "beta", "t"),
+              paramMargins=list(list(shape=2, scale=1),
+                                list(shape1=2, shape2=2),
+                                list(df=5)) )
```

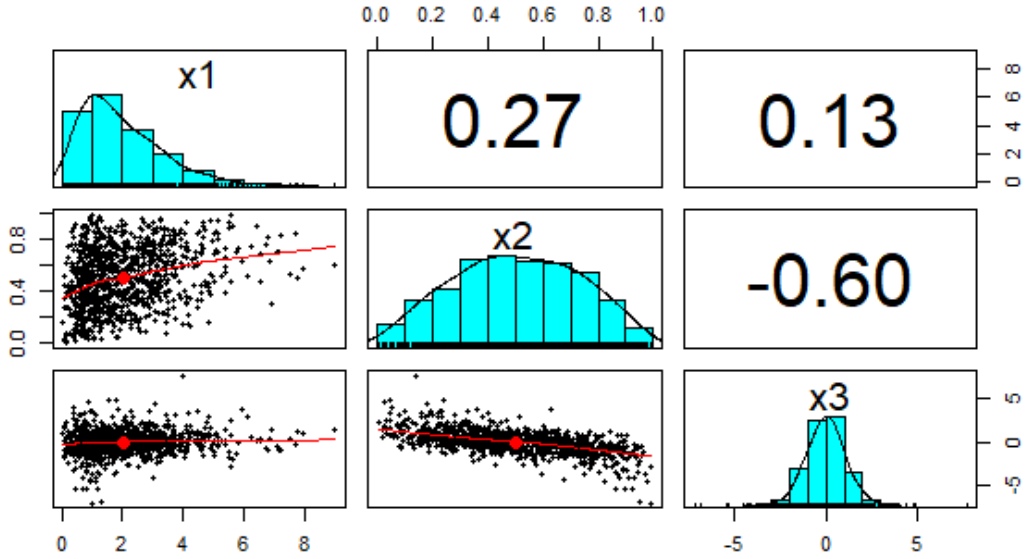
Ora che è stata specificata la struttura di dipendenza attraverso la copula (una copula normale) e impostato le marginali, la funzione mvdc[76]() genera la funzione di distribuzione desiderata, tramite la copula e i margini parametrici. Ora è possibile generare campioni casuali mediante il comando rmvdc[77] ().

```
> distcop<- rMvdc(1000, mvdcop)
> colnames(distcop) <- c("x1", "x2", "x3")
> pairs.panels(distcop)
```

[76] Multivariate Distributions Constructed from Copulas.
[77] Random mvdc.

Si ottengono così le correlazioni a coppie tramite la Copula

Figura 5.7: Grafico che descrive la correlazione a coppie tra le tre differenti distribuzioni marginali (Gamma, Beta e t-Student), utilizzando il metodo delle Copula.



5.3. SIMULAZIONE DEL PRICING TRAMITE IL METODO COPULA

Ora cerchiamo di illustrare l'approccio della copula per la determinazione del prezzo della cyber insurance utilizzando i dati del sondaggio fornitoci dall'ICSA (2005). Consideriamo un'ipotetica impresa I avente dati a livello di impresa relativi al numero dei computer interessati q e le perdite in dollari π per ogni principale virus informatico riscontrato nel 2004. Vengono considerate due violazioni all'anno ($\lambda = 2$). Supponiamo che il sistema IT dell'azienda non funzioni dopo la prima violazione e che il la richiesta di risarcimento venga pagata una sola volta, in tal modo la copertura è valida solo fino al verificarsi del primo evento di violazione e il periodo del contratto dura di conseguenza fino al verificarsi della prima violazione IT. Usiamo i dati del sondaggio ICSA (2005) per le reali incidenze di virus informatici e il numero effettivo di computer interessati, modificati e ridimensionati (in scala 1:100). Si osservi che, sia il numero di computer interessati, che il valore in dollari delle perdite sono eventi casuali. Il numero di computer interessati dipenderà da: la gravità del virus, la sicurezza dell'azienda e le politiche di sicurezza in atto; allo stesso modo, il valore in dollari delle perdite sarà casuale e nel raro caso dello stesso numero dei computer colpiti da due virus distinti, il grado di perdita non

sarà identico, perché dipenderà dalla capacità di ciascun virus di penetrare e danneggiare i computer e dal tipo di computer interessato. I dati sulla popolazione sono riportati nella figura 5.7.

Figura 5.7: Tabella che indica per ogni tipo di virus: il numero di computer q interessati e la perdita π in dollari che si è verificata.

	Virus	Numero q di computer interessati	Perdita π in dollari
1	Blaster	1291	355648.72
2	Slammer	849	339832.66
3	Sobig	238	115729.51
4	Klez	140	65090.38
5	Yaha	118	45402.25
6	Swen	108	66053.73
7	Dumaru	87	39182.88
8	Mimail	70	19556.82
9	Nachi	63	20087.13
10	Fizzer	58	20465.35
11	BugBear	50	10180.13
12	Lirva	47	11769.29
13	Sober	21	6944.48
14	Sircam	21	5339.08
15	Ganda	19	7547.77
Mean		212	75255
Standard deviation		363	114702

Fonte: ICSA Labs computer virus prevalence survey (Tippet, 2005)

Dopo aver ottenuto dalla ricerca ICSA (2005) i dati relativi al numero di computer colpiti da malware e le perdite associate, grazie al software statistico R analizzo queste due colonne di dati e la loro correlazione.

```
> qpc <- read.csv('qpc_r.csv',header=F)$V2
> perdite <- read.csv('perdite.csv',header=F)$V2
```

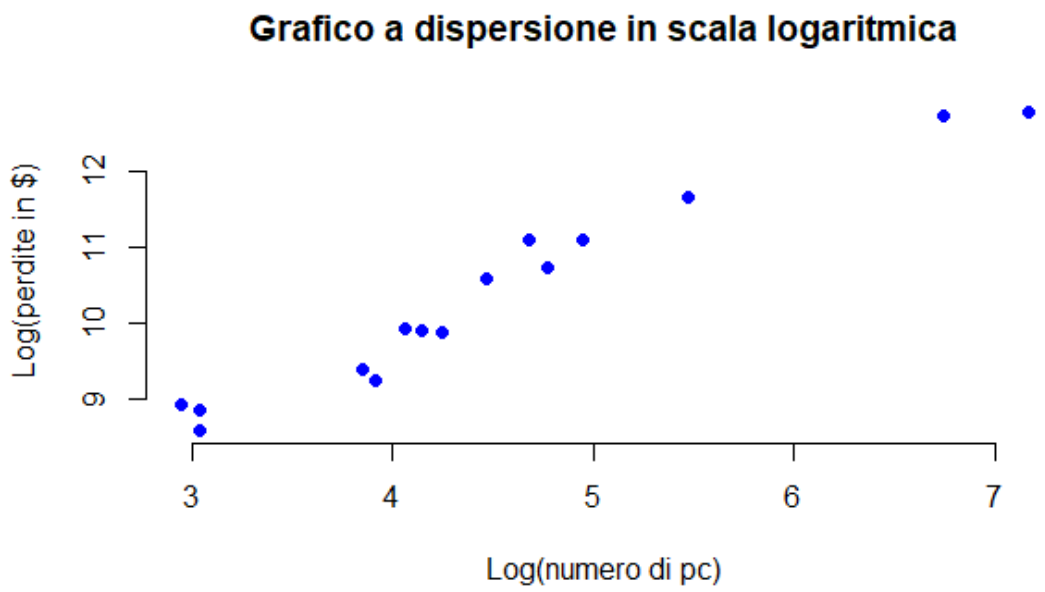
Dopo aver dichiarato la colonna del numero dei pc (qpc) e la colonna delle perdite in dollari (perdite) eseguo il comando summary per calcolare la media, mediana e i quantili delle due colonne.

```
> summary(qpc)
   Min. 1st Qu.  Median    Mean 3rd Qu.    Max.
   19.0    48.5    70.0   212.0   129.0  1291.0

> summary(perdite)
   Min. 1st Qu.  Median    Mean 3rd Qu.    Max.
   5339   10975   20465   75255   65572  355649
```

Trasformo in scala logaritmica le due variabili ed eseguo il comando per ottenere il grafico di dispersione.

Figura 5.8: Grafico di dispersione che mette in relazione, in scala logaritmica, il numero di pc interessati e le perdite avvenute.




```
> cor(qpc, perdite, method='spearman')
[1] 0.9597859
```

La correlazione, utilizzando il metodo di Spearman, è molto elevata, quindi il numero di computer interessato è fortemente correlato con l'ammontare delle perdite subite.

```
> library(VineCopula)
> u <- pobs(as.matrix(cbind(qpc,perdite)))[,1]
> v <- pobs(as.matrix(cbind(qpc,perdite)))[,2]
> qualecopula <- BiCopSelect(u,v,familyset=NA)
> qualecopula
```

Bivariate copula: Clayton (par = 10.67, tau = 0.84)

Tramite il pacchetto VineCopula, si simula la funzione che, ricerca la copula che si adatta in modo migliore ai nostri dati. Fondamentalmente la libreria VineCopula che consente di eseguire la selezione di copula usando BIC e AIC attraverso la funzione BiCopSelect ().

```
> m <- pobs(as.matrix(cbind(qpc,perdite)))
> fit.tau <- fitCopula(c.cop, m, method="itau")
> fit.tau
Call: fitCopula(copula, data = data, method = "itau")
Fit based on "inversion of Kendall's tau" and 15 2-dimensional observations.
Copula: claytonCopula
alpha
10.67
```

Quindi, dopo aver trovato nella Clayton Copula il miglior adattamento ai dati, usiamo il metodo itau per stimare il parametro di tale copula (alpha=10.67). Tramite il parametro della nostra Clayton Copula possiamo così andare a calcolare il tau e notare che, i due parametri erano già stati stimati con la funzione BiCopSelect.

```
> tau(claytonCopula(param = 10.67))
[1] 0.8421468
```

Copula di Clayton

Ci sono tre tipi di copula di Archimede: Clayton, Frank e Gumbel. La copula di Clayton, chiamata in questo modo proprio perché è stata introdotta da Clayton (1978), è una copula asimmetrica che mostra una maggiore dipendenza nella coda negativa che in quella positiva. Questa copula è data da:

$$C_\alpha(u,v) = max\left[(u^{-\alpha} + v^{-a} - 1)^{-\frac{1}{a}}, 0\right]; \qquad (5.8)$$

dove:

- α è il parametro della copula compreso nell'intervallo $(0, \infty)$. Se $a = 0$ allora le distribuzioni marginali sono indipendenti, quando $a \to \infty$ allora la copula di Clayton si avvicina al limite superiore di Fréchet-Hoeffding[78].

[78] Le copule ordinarie hanno un limite superiore naturale in tutte le dimensioni, il cosiddetto limite di Fréchet - Hoeffding, dopo il lavoro pionieristico di Wassily Hoeffding e più tardi, Maurice René Fréchet,

La dipendenza tra questa copula e la misura del rango tau di Kendall è semplicemente data da:

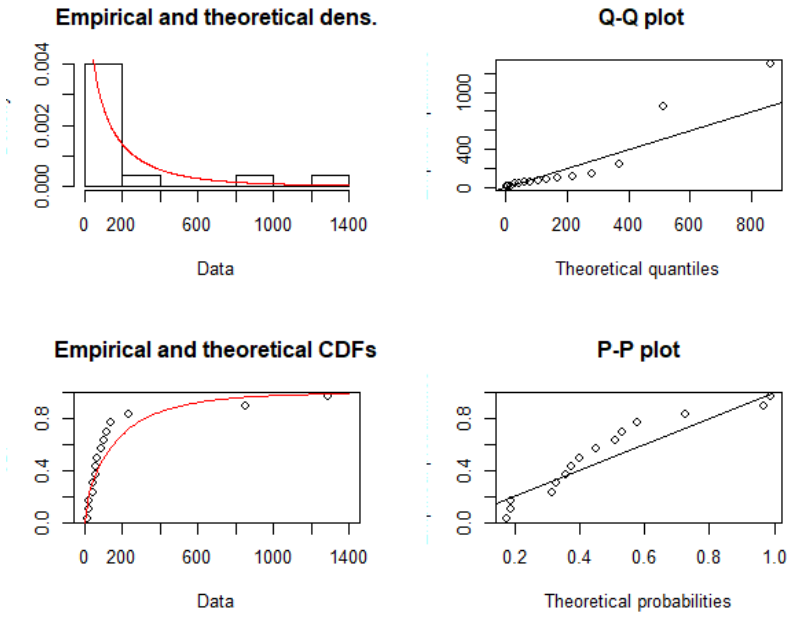
$$\tau_k = \frac{\alpha}{\alpha+2} \tag{5.9}$$

Come possiamo vedere dai seguenti grafici la distribuzione che meglio si adatta ai dati è la Weibull[79] (Rinne, 2008).

```
wdistqpc<-fitdist(qpc, "weibull")
> wdistqpc
Fitting of the distribution ' weibull ' by maximum likelihood
Parameters:
         estimate Std. Error
shape   0.7539872   0.137494
scale 170.2161609  62.099944

> plot(wdistqpc)
```

Figura 5.10. Grafici che mostrano come la distribuzione di Weibull meglio si adatti alla variabile qpc



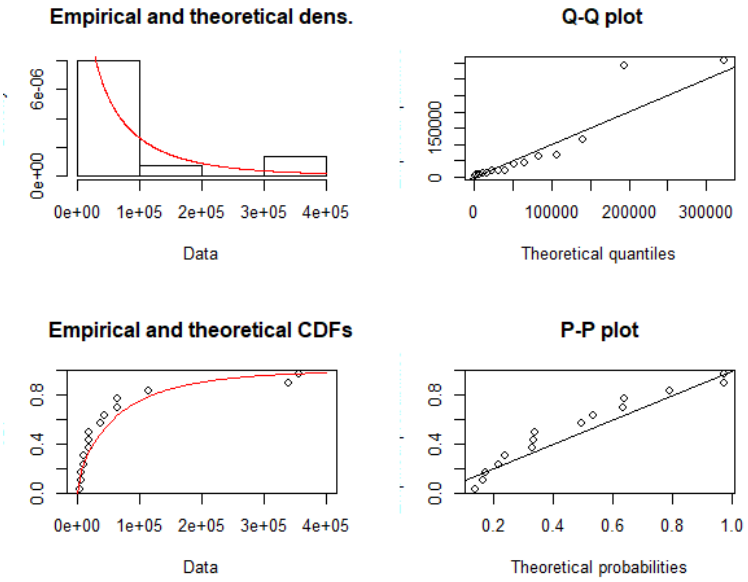

```
> wdistperdite<-fitdist(perdite, "weibull")
```

che lavorò in modo indipendente. A causa della restrizione sul parametro di dipendenza, il limite inferiore di Fréchet-Hoeffding non può essere raggiunto dalla copula di Clayton, ciò suggerisce che questo tipo di copula non può spiegare la dipendenza negativa (Embrechts et al., 2003).

[79] La distribuzione di Weibull è una distribuzione di probabilità continua definita su numeri reali positivi e descritta da due parametri: k parametro di forma e λ parametro di scala.

```
> wdistperdite
Fitting of the distribution ' weibull ' by maximum likelihood
Parameters:
          estimate   Std. Error
shape 7.621974e-01 1.391785e-01
scale 6.497487e+04 1.200765e+04
> plot(wdistperdite)
```

Figura 5.11. Grafici che mostrano come la distribuzione di Weibull meglio si adatti alla variabile perdite.



I quattro tipi di grafici rappresentati mostrano come la densità teorica della Weibull si adatti alla densità empirica, così come la funzione di distribuzione cumulata teorica. I due grafici a destra invece rappresentano il Q-Q plot, cioè la rappresentazione grafica dei quantili, e il P-P plot che traccia le probabilità e viene utilizzato per valutare la similitudine tra set di dati.

In seguito, andiamo a creare la distribuzione usando la copula di Clayton con parametro $\alpha = 10{,}67$, precedentemente identificata e utilizziamo come marginali le due distribuzioni di Weibull, che meglio si adattano ai nostri dati, cioè con parametri di forma e scala predefiniti.

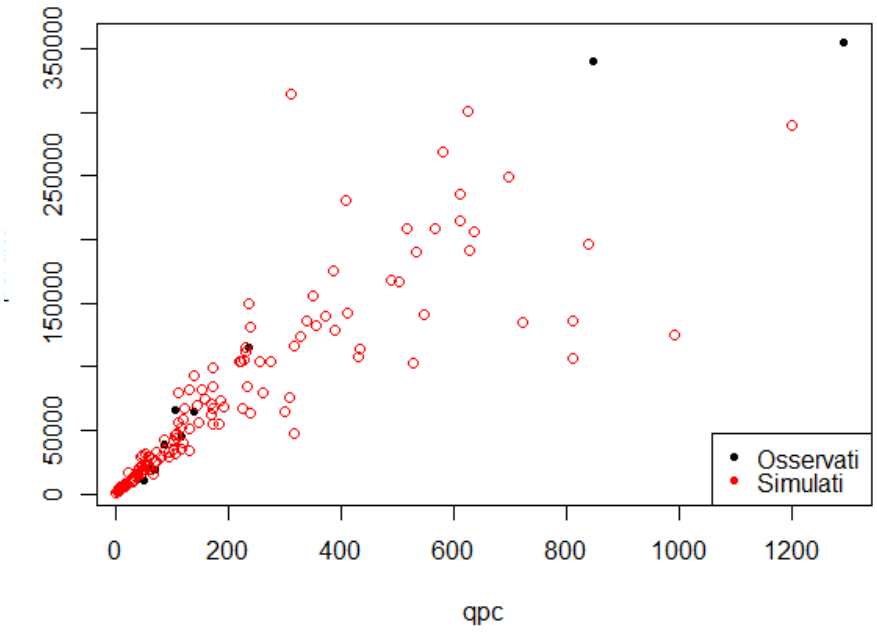
```
> copula_dist <- mvdc(copula=claytonCopula(10.67), margins=c("weibull","weibull"),
+ paramMargins=list(list(shape= 0.7539872, scale= 170.2161609),
+ list(shape= 7.621974e-01, scale= 6.497487e+04)))
> copula_dist
Multivariate Distribution Copula based ("mvdc")
```

```
 @ copula:
Clayton copula, dim. d = 2
Dimension:  2
Parameters:
  alpha   = 10.67
 @ margins:
[1] "weibull" "weibull"
   with 2 (not identical)  margins; with parameters (@ paramMargins)
List of 2
 $ :List of 2
  ..$ shape: num 0.7539872
  ..$ scale: num 170.2162
 $ :List of 2
  ..$ shape: num 0.7621974
  ..$ scale: num 64974.87
```

Con la funzione rMvdc si ottengono osservazioni simulate dalla distribuzione multivariata appena creata. Scelgo di simulare 150 volte la mia distribuzione e confronto con un semplice grafico di dispersione i risultati ottenuti.

```
> sim <- rMvdc(150, copula_dist)
> plot(qpc,perdite, pch=20)
> points(sim[,1],sim[,2],col='red', pch=21)
> legend('bottomright',c('Observed','Simulated'),col=c('black','red'),pch=20)
```

Figura 5.12. Grafico di dispersione dei dati che mette a confronto i dati osservati con i dati simulati presupponendo distribuzioni marginali Weibull e una Copula di Clayton per la struttura di dipendenza.



```
> cor(sim[,1],sim[,2],method='spearman')
[1] 0.9733144
```

La correlazione con il metodo Spearman, utilizzando la copula e adattando le due distribuzioni marginali a delle Weibull, è simile a quella trovata inizialmente (0.9597859).

Come è possibile notare, la copula di Clayton porta a risultati vicini alle osservazioni reali, anche se ci sono meno osservazioni estreme rispetto ai dati reali e vengono persi così alcuni dei risultati che potrebbero essere considerati outlier, ma nel contesto di cyber risk, sarebbe utile tenerli in considerazione . Se fossimo interessati a modellare il rischio associato, questa situazione sarebbe un grosso problema da affrontare con un'ulteriore calibrazione del modello. Il passo successivo è quello di utilizzare la simulazione appena ottenuta all'interno dell'equazione 4.13 in modo tale da ottenere una stima delle potenziali perdite:

$$\Pi = g(\pi, q) = \begin{cases} a_1 & se\ q < l \\ a_2 + \left(\frac{q-l}{q}\right)\left(\frac{\pi}{10}\right) & se\ l \leq q < m \\ a_3 + \left(\frac{q-m}{q}\right)\left(\frac{\pi}{10}\right) & se\ q \geq m \end{cases}$$

dove

- $a_1 = 400$, $a_2 = 125$, $a_3 = 300$ e sono costanti
- $l = 10$ e rappresenta il limite inferiore del numero di computer/server
- $m = 500$ e rappresenta il limite superiore del numero di computer/server

Tramite un ciclo for, dopo aver simulato 10000 volte, trovo il mio vettore di potenziali perdite:

```
> pp<-array()
> for(i in 1:10000){
+ if(sim[i]<10) {pp[i]<-400}
+ else if(sim[i]<50) {pp[i]<-125+((sim[i]-10)/sim[i])*(sim[i,2]/10)}
+ else {pp[i]<-300+((sim[i]-50)/sim[i])*(sim[i,2]/10)}
+ }
> pp
```

Dopo aver ottenuto il vettore delle potenziali perdite, il passo successivo è quello di calcolare il premio, utilizzando la formula:

$$C = \omega e^{-rT} P$$

- ω è una variabile binaria, uguale a 1 (con probabilità 0,052[80]) se l'evento coperto si verifica e 0 (con probabilità 0,948) altrimenti;
- T è il tempo fino all'incidente della violazione della sicurezza, stimato di 197 giorni[81];
- r è il tasso di sconto, (4,033 %)[82] e
- P è l'importo pagato dalla compagnia assicurativa in caso di violazione, che nel nostro caso equivale alla perdita potenziale

```
> vett_premio_2005<-0.052*pp*exp(x=-197/365*0.04033)
> mean(vett_premio_2005)
[1] 319.7866
```

Computando 10000[83] volte questa formula e successivamente calcolando la media, si trova come risultato 320, che rappresenta l'ammontare medio in dollari del premio per ciascun computer.

Polizza di secondo tipo: polizza per danni di prima parte con franchigia.

In questo caso non vale più l'uguaglianza $P = \Pi$ ma, fissata una franchigia d, si calcola l'importo pagato P tramite la formula 4.17 riportata qui di seguito.

$$P = \begin{cases} 0 & se\ \Pi \leq d \\ \Pi - d & se\ \Pi > d \end{cases}$$

Con R calcolo l'importo pagato P tramite un ciclo for assegnando alla franchigia i seguenti valori: 500, 1000, 1500, 2000, 2500;

```
> pp2005_2<-array()
d<-500
> for(i in 1:10000){
+ if(pp[i]<=d) {pp2005_2[i]<-0}
+ else {pp2005_2[i]<-pp[i]-d}
}
```

Procedo con il passo successivo e calcolo il premio come per la polizza di tipo 1.

[80] Tale probabilità è stata ricavata dal report "Cybercrime against business" (Bureau of justice statistics, 2005)

[81] Dato estrapolato dallo studio di Ponemon institute "Cost of Data Breach Study:Impact of BusinessContinuity Management" (Ponemon L. 2018).

[82] Media del tasso Libor americano a 12 mesi nel 2005.

[83] Tante volte quante sono le righe del vettore di perdite potenziali.

$$C = \omega e^{-rT} P$$

```
vett_premio_2005_2<-0.052*pp2005_2*exp(x=-197/365*0.04033)
> mean(vett_premio_2005_2)
[1] 295.7176
```

Nella seguente tabella riporto i risultati ottenuti.

Franchigia	0	500	1000	1500	2000	2500
Ammontare medio del premio in dollari	320	296	277	261	247	234

Polizza di terzo tipo: polizza per danni di prima parte con coassicurazione e limite: fissando la franchigia *d*, la coassicurazione di *a* e un limite di *k* è possibile calcolare il premio per la polizza di terzo tipo. L'assicurazione non paga nulla quando la perdita è inferiore a *d*, paga il 100% *(1 - a)* delle perdite in eccesso rispetto a *d*, ma non paga mai nulla in eccesso. La relazione tra la variabile casuale di interesse P e la variabile casuale osservata Π è data dall'equazione 4.18, quindi:

$$P = \begin{cases} 0, & se\ \Pi \leq d \\ (1-a)(\Pi - d), & se\ d < \Pi < d + \frac{k}{1-a} \\ k\ , & se\ \ \Pi > d + \frac{k}{1-a} \end{cases}$$

Con il software statistico R è possibile calcolare l'importo pagato P tramite un ciclo for assegnando:

- alla franchigia i seguenti valori: 500, 1000, 1500, 2000, 2500;
- alla percentuale di coassicurazione a i valori: 10%, 15%, 20%, 25%;
- al limite k i valori: 10000, 15000, 20000, 25000.

Quindi tramite il ciclo for

```
pp2005_3<-array()
for(i in 1:10000){
if(pp[i]<=d) {pp2005_3[i]<-0}
else if(pp[i]<d+k/(1-a)) {pp2005_3[i]<-(1-a)*(pp[i]-d)}
else {pp2005_3[i]<-k}
}
```

Procedo con il passo successivo e calcolo il premio come per la polizza di tipo 1.

```
vett_premio_2005_3<-0.052*pp2005_3*exp(x=-197/365*0.04033)
mean(vett_premio_2005_3)
```

Riporto i risultati ottenuti nella seguente tabella

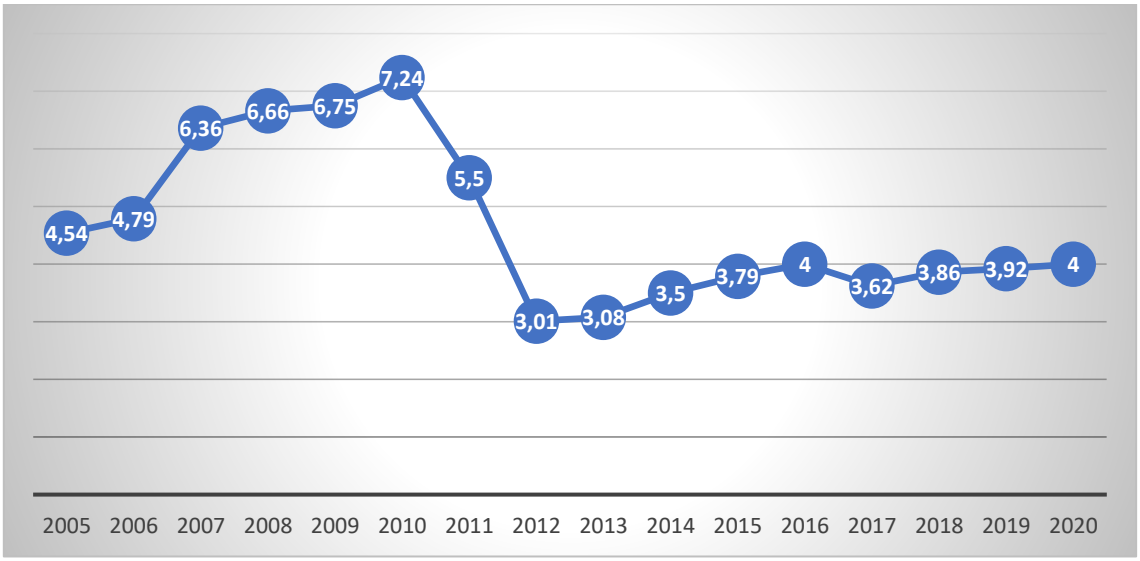
		Franchigia	0	500	1000	1500	2000	2500
	a=10%	Premio	198	181	168	157	148	139
	a=15%	Premio	192	176	163	153	144	136
k=10000	***a=20%***	Premio	186	170	158	148	139	131
	a=25%	Premio	179	164	152	143	134	127
	a=10%	Premio	234	215	200	187	177	168
	a=15%	Premio	225	207	192	181	170	161
k=15000	***a=20%***	Premio	216	198	185	173	164	155
	a=25%	Premio	206	189	177	166	156	148
	a=10%	Premio	254	234	218	205	193	183
	a=15%	Premio	243	224	209	196	185	175
k=20000	***a=20%***	Premio	232	214	200	188	177	167
	a=25%	Premio	220	203	190	178	168	159
	a=10%	Premio	266	246	229	216	204	193
	a=15%	Premio	254	234	219	206	195	184
k=25000	***a=20%***	Premio	241	223	208	196	185	175
	a=25%	Premio	228	211	197	185	175	166

È possibile notare che, l'ammontare del premio è direttamente proporzionale con l'ammontare del limite k e quello della franchigia *d*, mentre è inversamente proporzionale alla percentuale *a* di coassicurazione. L'ammontare minimo del premio è 127 in corrispondenza di un limite *k* di 10000, coassicurazione *a* del 25% e franchigia *d* 2500 dollari; l'importo massimo del premio viceversa è 266 dollari in corrispondenza del limite *k* di 25000, coassicurazione *a* di 10% e con zero franchigia.

5.3.1 CONFRONTO CON I DATI DEL 2018

Attraverso un confronto, sarebbe possibile calcolare il premio per la cyber insurance, riferendosi alle numerose ricerche svolte dall'istituto Ponemon (2019) riguardanti appunto le violazioni dei dati, il loro impatto e il costo medio annuale. Grazie a tali studi, svolti anno dopo anno, è possibile notare che il costo medio globale annuo riguardante le violazioni per le imprese dal 2005 al 2020 ha subito un brusco calo nel 2011 e successivamente nel 2012 rispettivamente del 32% e del 82 % per risalire e stabilizzarsi a 3.92 milioni nel 2019; nel 2020 si prevede che questo costo medio continuerà ad aumentare sfiorando i 4 milioni.

Figura 5.13. Andamento del costo medio annuo della violazione di dati a livello globale e misurata in milioni di dollari.



Fonte: Cost of a Data Breach Report, (Ponemon Institute, 2019).

Per stimare il premio annuo della cyber insurance per il 2019, ho fatto riferimento ad una tabella di richieste di liquidazione contenuta nel "Cyber Claims Report" a cura di Net Diligence (O'Connor C. 2019). Ogni richiesta di liquidazione viene suddivisa per tipologia di "problema" riscontrato e tutte rappresentano l'ammontare di perdita totale.

Figura 5.14. Prospetto rappresentante il tipo di richiesta di liquidazione comprendente il numero di computer interessati e l'ammontare di perdita sopportata in dollari.

	Computer interessati (qpc)	Perdite subite π in dollari
Compromissione di email di lavoro	164	25.6 M
Hackeraggio	285	96.1 M
Azione legale da parte di terze parti	112	27 M
Smarrimento di laptop o altri device	95	7.2 M
Malware/virus	142	43.7 M
Negligenza	7	0.4 M
Dati cartacei	23	1.6 M
Phishing	133	10.6 M
Errori di programmazione	24	7.3 M
Ransomware	478	71.6 M
Dipendenti delinquenti	80	12.1 M
Ingegneria sociale	547	58.6 M
Errori da parte dello staff	120	9.4 M
Problemi tecnici	10	19.3 M
Cyber furto	9	1.1 M
Infrazione del copyright	9	1.3 M
Frodi	106	19.1 M
Raccolta errata dei dati	1	86 K

Fonte: Cyber Claims Report (O'Connor, 2019).

Tramite la ricerca della NetDiligence (2019) ho ricavato i dati relativi al numero di computer colpiti dal cyber crime, nonché da problemi tecnici, da errori e le perdite ad essi associate. Grazie all'ausilio del software statistico R sono stato in grado di analizzare i dati e la loro correlazione.

```
> qpc2018 <- read.csv('qpc2018_r.csv',header=F)$V2
> perdite2018 <- read.csv('perdite2018_r.csv',header=F)$V2
```

Successivamente calcolo mediante il comando summary la media, la mediana e i quantili per ciascuna delle due variabili; con il comando sd invece computo la deviazione standard.

```
> summary(qpc2018)
   Min. 1st Qu.  Median    Mean 3rd Qu.    Max.
   1.00   13.25  100.50  130.28  139.75  547.00

> summary(perdite2018)
   Min. 1st Qu.  Median    Mean 3rd Qu.    Max.
    344   12000   45400   91575  106600  384400
```

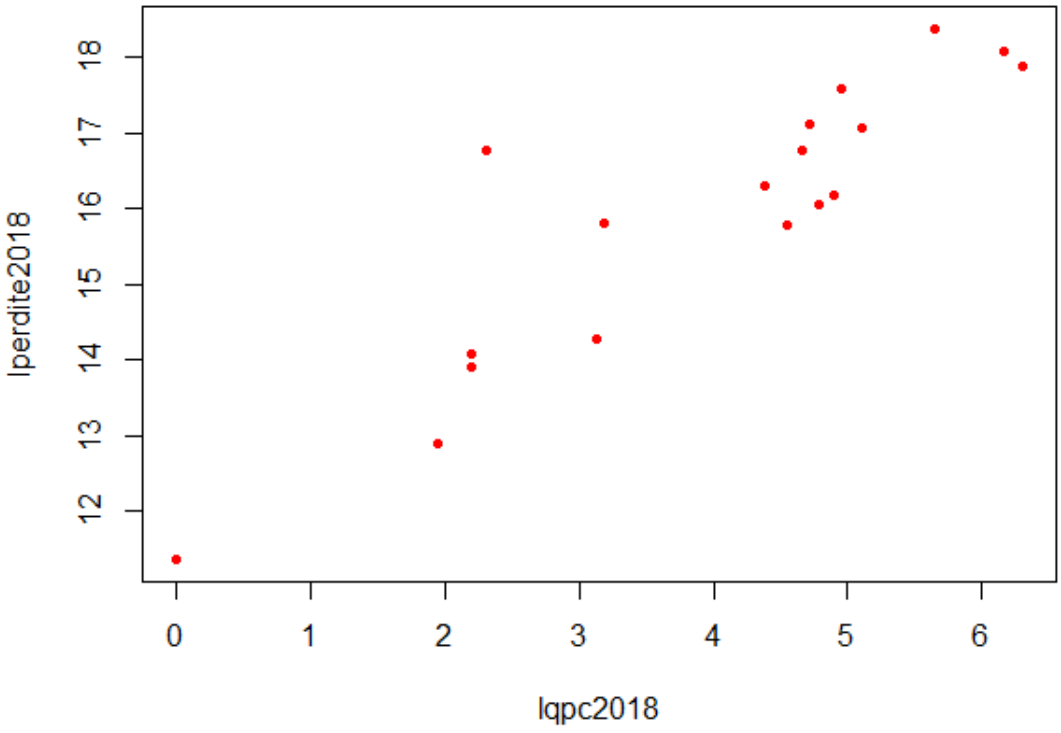
```
> sd(qpc2018)
[1] 157.7764

> sd(perdite2018)
[1] 109976.
```

Noto che il valore assoluto della deviazione standard per le mie due variabili è molto elevato.

```
> lqpc2018=log(qpc2018)
> lperdite2018=log(perdite2018)
> plot(lqpc2018,lperdite2018, col="red", pch=20)
```

Figura 5.15: Grafico di dispersione che mette in relazione, in scala logaritmica, il numero di pc interessati e le perdite avvenute per il 2018.




```
> cor(qpc2018,perdite2018,method='spearman')
[1] 0.877646
```

La correlazione con il metodo Spearman è molto meno marcata rispetto al 2005.

```
> library(VineCopula)
> u <- pobs(as.matrix(cbind(qpc2018,perdite2018)))[,1]
```

```
> v <- pobs(as.matrix(cbind(qpc2018,perdite2018)))[,2]
> qualecopula <- BiCopSelect(u,v,familyset=NA)
> qualecopula
Bivariate copula: Joe (par = 3.675, tau = 0.59)
```

La copula Joe

La copula Joe, introdotta da Joe nel 1993, assume la seguente forma (Embrechts et al., 2003):

$$C_\alpha(u,v) = 1 - [(1-u)^\alpha + (1-v)^a - (1-u)^a(1-v)^\alpha]^{\frac{1}{\alpha}}; \quad (5.10)$$

dove:

- Il parametro a della copula è compreso nell'intervallo $[1,\infty)$ e, come per copula di Clayton, non è possibile spiegare la dipendenza negativa; infatti, la copula raggiunge il limite superiore di Frèchet per $\alpha \to \infty$, ma non può raggiungere il limite inferiore.

La relazione tra il parametro a della copula di Joe e τ inoltre, non ha un'espressione in forma chiusa, ma assume la seguente forma:

$$\tau = \int_{t\_^0}^{1} \frac{[ln(1-t^a)](1-t^a)}{t^{\alpha-1}} dt \quad (5.11)$$

τ è compreso tra 0 e 1 e l'indipendenza corrisponde a $\alpha = 1$.

```
> m <- pobs(as.matrix(cbind(qpc2018,perdite2018)))
> j.cop<-joeCopula(dim=2)
> fit <- fitCopula(j.cop, m, method="mpl")
> fit
Call: fitCopula(copula, data = data, method = "mpl")
Fit based on "maximum pseudo-likelihood" and 18 2-dimensional observat
ions.
Copula: joeCopula
alpha
3.675
The maximized loglikelihood is 9.406
Optimization converged
> fit <- fitCopula(j.cop, m, method="ml")
> fit
Call: fitCopula(copula, data = data, method = "ml")
Fit based on "maximum likelihood" and 18 2-dimensional observations.
Copula: joeCopula
alpha
```

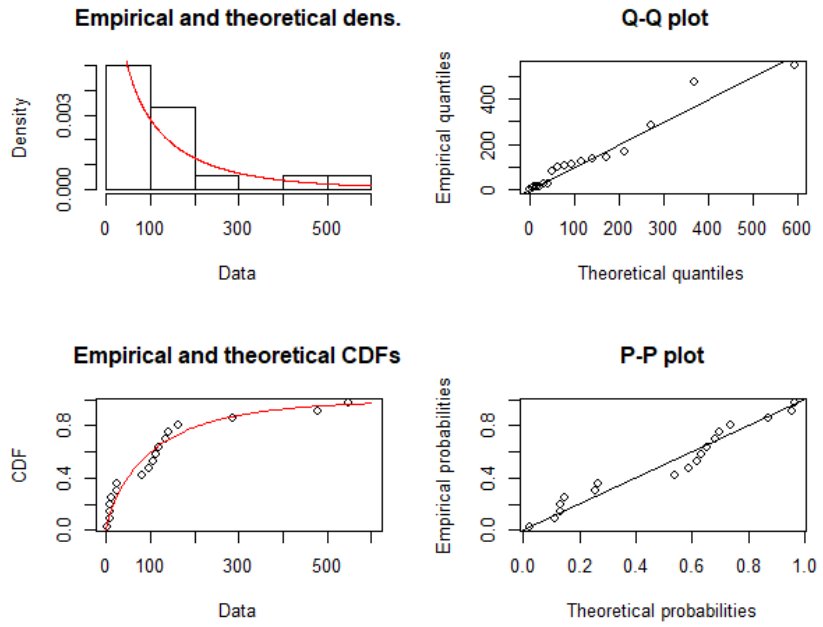
```
3.675
The maximized loglikelihood is 9.406
Optimization converged
> coef(fit)
   alpha
3.675325

> tau(joeCopula(param = 3.675325))
[1] 0.5871925
```

In questo caso il tipo di Copula che meglio si adatta ai nostri dati è la Copula di Joe; usiamo quindi il metodo ml per stimare il parametro di tale copula (e non il metodo itau come con i dati del 2005). Tramite il parametro della nostra Joe Copula ($\alpha = 3{,}675325$), possiamo così andare a calcolare il tau e notare che, come nel caso della copula di Clayton, i due parametri erano già stati stimati con la funzione BiCopSelect.

```
> wdistqpc2018<-fitdist(qpc2018, "weibull")
> wdistqpc2018
Fitting of the distribution ' weibull ' by maximum likelihood
Parameters:
         estimate Std. Error
shape   0.7647506  0.1438226
scale 111.9047194 36.3285424
plot(wdistqpc2018)
```

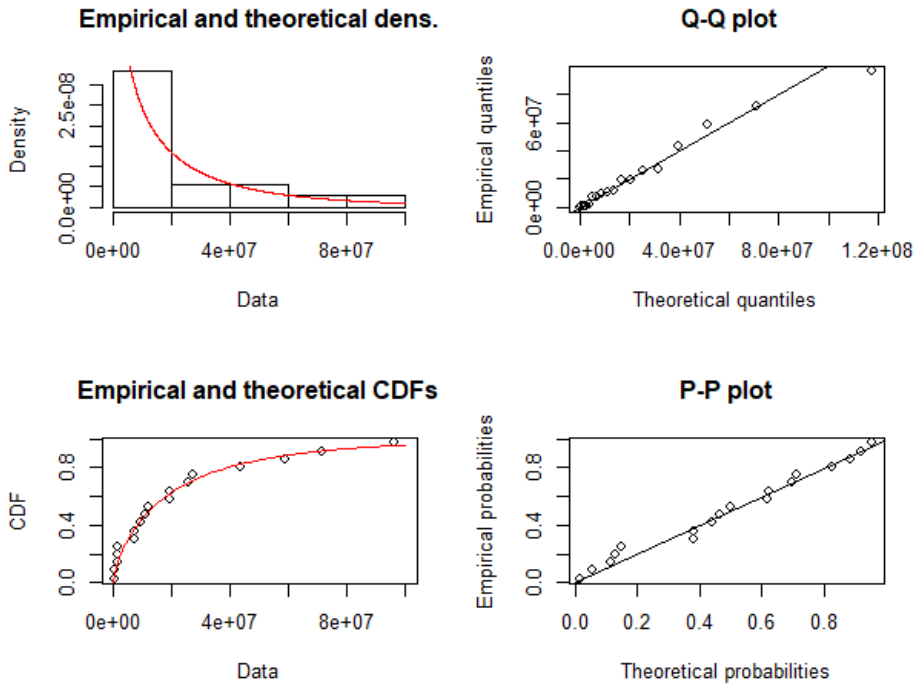
Figura 5.16. Grafici che mostrano come la distribuzione di Weibull meglio si adatti alla variabile qpc2018.



```
> wdistperdite2018<-fitdist(perdite2018, "weibull")
> wdistperdite2018
Fitting of the distribution ' weibull ' by maximum likelihood
Parameters:
          estimate   Std. Error
shape 7.137813e-01  0.1332965
scale 7.518842e+04  8388.6083823

> plot(wdistperdite2018)
```

Figura 5.17. Grafici che mostrano l'adattamento della distribuzione di Weibull alla variabile perdite2018.



I quattro grafici per le variabili del 2018, così come quelle del 2005 mostrano come la densità teorica della Weibull si adatti alla densità empirica, e come la funzione di distribuzione cumulata teorica si adatti alla controparte empirica. L'adattamento si denota anche dal grafico dei quantili e da quello delle probabilità.In seguito, andremo a plasmare la distribuzione mediante la copula di Joe con parametro $\alpha = 3{,}675$, precedentemente identificata e utilizzando come marginali le due distribuzioni di Weibull, che meglio si adattano ai nostri dati, cioè con parametri di forma e scala predefiniti.

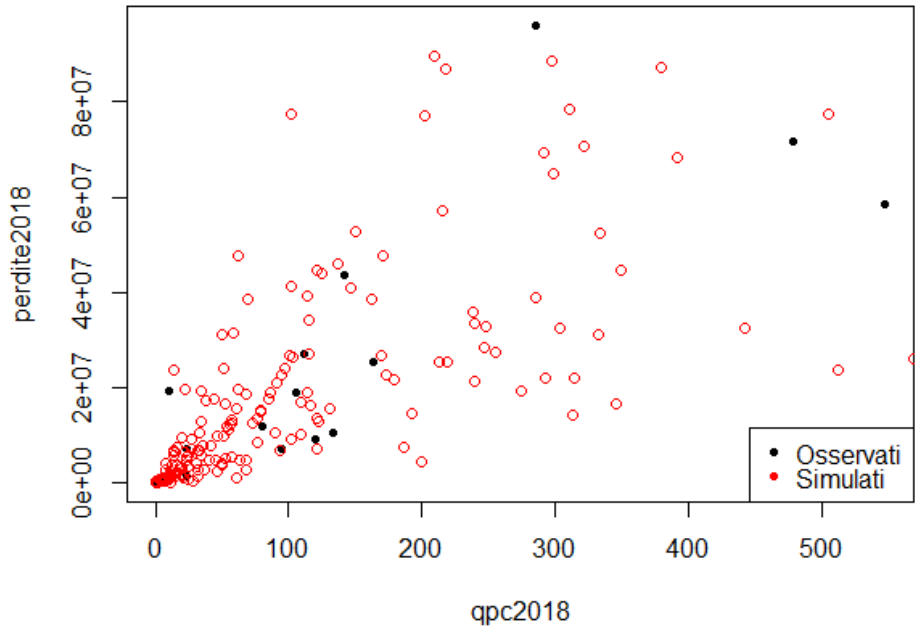
```
> copula_dist2018 <- mvdc(copula=claytonCopula(3.67), margins=c("weibu
ll","weibull"),
+ paramMargins=list(list(shape= 0.7647506, scale= 111.9047194),
+ list(shape= 7.137813e-01, scale= 7.518842e+04)))
```

```
> copula_dist2018
Multivariate Distribution Copula based ("mvdc")
 @ copula:
Clayton copula, dim. d = 2
Dimension:  2
Parameters:
  alpha   = 3.67
 @ margins:
[1] "weibull" "weibull"
   with 2 (not identical)  margins; with parameters (@ paramMargins)
List of 2
 $ :List of 2
  ..$ shape: num 0.7647506
  ..$ scale: num 111.9047
 $ :List of 2
  ..$ shape: num 0.7137813
  ..$ scale: num 75188.42


> sim2018<-rMvdc(180, copula_dist2018)
> plot(qpc2018,perdite2018, pch=20)
> points(sim2018[,1],sim2018[,2],col='red', pch=21)
> legend('bottomright',c('Osservati','Simulati'),col=c('black','red'),
pch=20)
```

Con la funzione rMvdc si ottengono osservazioni simulate dalla distribuzione multivariata appena creata. Scelgo di simulare 180 volte la mia distribuzione e confronto con un semplice grafico di dispersione i risultati ottenuti.

Figura 5.18. Grafico di dispersione dei dati che mette a confronto i dati osservati con i dati simulati presupponendo distribuzioni marginali Weibull e una Copula di Joe per la struttura di dipendenza.




```
> cor(sim2018[,1],sim2018[,2],method='spearman')
[1] 0.8622139
```

La correlazione con il metodo Spearman, utilizzando la copula e adattando le due distribuzioni marginali a delle Weibull è simile a quella trovata inizialmente (0.877646).

Come è possibile notare, la copula di Joe porta a risultati vicini alle osservazioni reali, ci sono molte osservazioni estreme che non rispecchiano i dati empirici, fatto comunque positivo dato che, nel contesto di cyber risk, è utile tenere in considerazione anche i cosiddetti outlier.

Tramite il ciclo for, dopo aver simulato 10000 volte, trovo il mio vettore di potenziali perdite:

```
> pp2018<-array()
> for(i in 1:10000){
+ if(sim2018[i]<10) {pp2018[i]<-400}
+ else if(sim2018[i]<50)
{pp2018[i]<-125+((sim2018[i]-10)/sim2018[i])*(sim2018[i,2]/10)}
+ else {pp2018[i]<-300+((sim2018[i]-50)/sim2018[i])*(sim2018[i,2]/10)}
+ }
> pp2018
```

Dopo aver ottenuto il vettore delle potenziali perdite, il passo successivo è quello di calcolare il premio, utilizzando la formula:

$$C = \omega e^{-rT} P$$

- ω è una variabile binaria, uguale a 1 (con probabilità 0,0832[84]) se l'evento coperto si verifica e 0 (con probabilità 0,9168) altrimenti;
- T è il tempo fino all'incidente della violazione della sicurezza, stimato di 197 giorni[85];
- r è il tasso di sconto, (2 %)[86] e
- P è l'importo pagato dalla compagnia assicurativa in caso di violazione, che nel nostro caso equivale alla perdita potenziale.

```
> vett_premio_2018<-0.0832*pp2018*exp(x=-197/365*0.02)
> mean(vett_premio_2018)
[1] 542.1585
```

Computando quindi tante volte, quante sono le righe del mio vettore di potenziali perdite, calcolo il valore atteso ottenendo come risultato 542, che rappresenta l'ammontare medio in dollari del premio per ciascun computer. Noto fin da subito che, questo valore è molto più elevato rispetto a quello trovato per i dati del 2005 (questa media è salita dell'69.38 %) e questa crescita è dovuta sia all'incremento del tasso di infezione (da 5.2% è salito all'8.32%), che all'inasprimento dei cyber attack, i quali causano danni maggiori rispetto al passato[87].

Polizza di secondo tipo: polizza per danni di prima parte con franchigia.
Con R calcolo l'importo pagato P tramite un ciclo for assegnando alla franchigia i seguenti valori: 500, 1000, 1500, 2000, 2500;

```
pp2018_2<-array()
for(i in 1:10000){
if(pp2018[i]<=d) {pp2018_2[i]<-0}
else {pp2018_2[i]<-pp2018[i]-d}
}
```

[84] Tale probabilità è stimata dal report "The missing report" (Taylor, 2018)
[85] Dato estrapolato dallo studio di Ponemon institute "Cost of Data Breach Study:Impact of Business Continuity Management" (Ponemon institute, 2018).
[86] Tasso FED datato 13 giugno 2018.
[87] Ho potuto ricavare tale informazione tramite il calcolo la media delle potenziali perdite che, da 7429 $ nel 2005, passa a 8620 $ nel 2018 (quindi un incremento del 16%).

Procedo con il passo successivo e calcolo il premio come per la polizza di tipo 1.

$$C = \omega e^{-rT} P$$

```
> vett_premio_2018_2<-0.0832*pp2018_2*exp(x=-197/365*0.02)
> mean(vett_premio_2018_2)
[1] 401.2652
```

Nella seguente tabella riporto i risultati ottenuti per l'anno 2018.

Franchigia	**0**	**500**	**1000**	**1500**	**2000**	**2500**
Ammontare medio del premio in dollari	542 (+69.4%)	503 (+ 70%)	473 (+ 70..1%)	447 (+ 71.3%)	423 (+71.3%)	401 (+71.4%)

Quindi il premio della polizza del secondo tipo, cioè comprendente di franchigia, è aumentato in media del 70.6% rispetto al 2005.

Polizza di terzo tipo: polizza per danni di prima parte con coassicurazione e limite: fissando la franchigia *d*, la coassicurazione di *a* e un limite di *k*. Grazie al software statistico R è quindi possibile procedere al calcolo dell'importo pagato P tramite un ciclo for assegnando:

- alla franchigia i seguenti valori: 500, 1000, 1500, 2000, 2500;
- alla percentuale di coassicurazione a i valori: 10%, 15%, 20%, 25%;
- al limite k i valori: 10000, 15000, 20000, 25000.

```
pp2018_3<-array()
for(i in 1:10000){
if(pp2018[i]<=d) {pp2018_3[i]<-0}
else if(pp2018[i]<d+k/(1-a)) {pp2018_3[i]<-(1-a)*(pp2018[i]-d)}
else {pp2018_3[i]<-k}
}
vett_premio_2018_3<-0.0832*pp2018_3*exp(x=-197/365*0.02)
mean(vett_premio_2018_3)
```

Procedo con il passo successivo e calcolo il premio come per la polizza di tipo 1.

```
vett_premio_2018_3<-0.0832*pp2018_3*exp(x=-197/365*0.02)
mean(vett_premio_2018_3)
```

Riporto i risultati ottenuti nella seguente tabella

		Franchigia	0	500	1000	1500	2000	2500
k=10000	a=10%	Premio	320	292	271	253	238	224
	a=15%	Premio	311	284	264	247	232	218
	a=20%	Premio	301	275	256	239	225	212
	a=25%	Premio	290	265	247	231	218	205
k=15000	a=10%	Premio	380	350	326	306	289	273
	a=15%	Premio	367	337	315	296	279	263
	a=20%	Premio	352	324	303	285	268	254
	a=25%	Premio	337	311	291	273	258	244
k=20000	a=10%	Premio	418	385	361	339	320	303
	a=15%	Premio	401	370	346	326	308	291
	a=20%	Premio	383	354	331	312	294	279
	a=25%	Premio	364	337	316	297	281	266
k=25000	a=10%	Premio	441	408	382	360	340	322
	a=15%	Premio	422	390	366	344	325	308
	a=20%	Premio	401	371	348	328	310	294
	a=25%	Premio	380	352	330	311	294	279

L'ammontare minimo del premio è 224 in corrispondenza di un limite *k* di 10000, coassicurazione *a* del 25% e franchigia *d* ammontante a 2500 dollari; l'importo massimo del premio viceversa è 441 dollari in corrispondenza del limite *k* di 25000, coassicurazione *a* di 10% e con zero franchigia. Rispetto al premio calcolato con i dati del 2005, si può facilmente notare che, nel 2018 il premio per la polizza di tipo 3 è aumentato mediamente del 61%.

CONCLUSIONI

Con la stesura di questa tesi, mi sono prefissato di fornire un quadro generale dei principali modelli di simulazione e pricing del cyber security risk al fine di ottenere così l'ammontare del premio della copertura cyber.

Ho scelto di focalizzare l'attenzione sull'utilizzo delle funzioni Copula, strumenti estremamente efficaci nel momento in cui si modella il comportamento congiunto di variabili casuali, tuttavia è facile confonderle, trascurando aspetti importanti del fenomeno che si sta tentando di modellare. L'autentico potere delle copule è quello di generalizzare la modellizzazione del comportamento congiunto di molteplici variabili casuali in modo semplice attraverso l'approccio "*divide et impera"* per le marginali e la struttura di dipendenza. Un altro fattore che viene spesso trascurato riguarda la struttura delle dipendenze, che non si presenta sempre fissa, ma spesso potrebbe variare nel tempo; tale problema non è compreso nelle copule, mentre meriterebbe un'attenzione particolare nel momento in cui si eseguono le simulazioni.

Cercando di applicare il modello ai miei dati per mezzo delle funzioni Copula, ho avvertito anche io, come Herath T. ed Herath H. (2011) nel loro studio "Cyber-Insurance: Copula Pricing Framework and Implications for Risk Management", il principale limite nel pricing della cyber insurance, cioè l'insufficienza di dati su: l'ammontare delle perdite associate ai cyber attack e l'intervallo di tempo che mediamente intercorre da quando si manifesta un virus/malware al momento in cui esso viene scoperto; problema ulteriormente acuito dal fatto che le imprese sono restie a rivelare dettagli relativi a violazioni della sicurezza. Avendo un maggior numero di dati, infatti, sarebbe possibile determinare in modo più accurato il tipo di copula che meglio si adatta alle distribuzioni marginali.

Un ulteriore ostacolo, oltre alla quantità di dati, riguarda la qualità di essi: è più probabile che π dipenda dal numero e dal tipo di vulnerabilità, che potrebbe a sua volta dipendere dalle precauzioni di sicurezza adottate dall'azienda e dall'educazione alla cyber security acquisita.

Qualora si verificasse un incidente, le perdite dipenderanno dal tipo di computer interessato e dall'utente, oltre che dal tipo di malware che ha causato l'incidente; un ransomware o un attacco Denial of Service comportano una percentuale di successo maggiore rispetto al semplice phishing. Il tempo necessario per accertare di essere stati

vittima di un malware è molto variabile e dipende dal livello di sicurezza informatica di cui è dotata un'impresa, ma anche e soprattutto dal tipo di cyber attack sofferto (un ransomware viene scoperto tempestivamente, perché basato su richieste di riscatto, mentre nel caso di violazioni di dati potrebbero volerci anni).

Infine, una complicazione rilevante del modello delle sorelle Herath (2011), implica la mancanza di distinzione tra le grandi e piccole e medie imprese, in quanto, i cyber attack si concentrano sul secondo tipo, ipotizzando che queste non dispongano di un'efficiente sicurezza informatica, di conseguenza il tentativo di aggressione va a buon fine. Contrariamente, le grandi imprese, maggiormente preparate, subiscono un numero davvero esiguo di cyber attack, ma ognuno di essi causa perdite di straordinario spessore, anche di decine di milioni di dollari.

Secondo il mio parere, la ricerca futura implica ampi spazi di crescita e miglioramento.

È indispensabile riconoscere la necessità di affidarsi ad una seria raccolta di dati, sia dal punto di vista quantitativo che qualitativo. Le imprese dovrebbero concentrarsi e fornire risposte accurate nei sondaggi proposti, in modo tale che le compagnie assicurative possano in futuro somministrare dei premi più precisi e personalizzati, frutto di calcoli più scrupolosi.

BIBLIOGRAFIA

[1] Accenture (2019), *Ninth Annual Cost of Cybercrime Study*, disponibile a https://www.accenture.com/us-en/insights/security/cost-cybercrime-study;

[2] Accenture Security (2019), *Cyber Threatscape Report 2019*, disponibile a https://www.accenture.com/_acnmedia/pdf-107/accenture-security-cyber.pdf;

[3] Allen, L.J.S., (1994), Some discrete-time *SI*, *SIR*, and *SIS* epidemic models, *Mathematical Biosciences,* Vol. 124, No.1, pp. 83-105;

[4] Ane, T. e Kharoubi C., (2003), Dependence Structure and Risk Measure, The Journal of Business, Vol. 76, No. 3, pp. 411-438;

[5] Antonucci, D., (2017), *The Cyber Risk Handbook. Creating and Measuring Effective Cybersecurity Capabilities*, Wiley Finance, s.l. 1. edizione;

[6] Arnold, S., Triantafyllou, C., Sawyer, A., Hofmann, S., Gabrieli, J. e Whitfield-Gabrieli, S., (2013), Hyper-Connectivity of Subcortical Resting. State Networks in Social Anxiety Disorder, *Brain Connectivity*, Vol. 4, No. 2, pp. 81-90;

[7] Arrow, K., (1964), The Role of Securities in the Optimal Allocation of Risk Bearing, *The Review of Economic Studies, Vol. 31, No. 2, pp. 91-96;*

[8] Backus, D., Chernov, M. e Martin, I., (2011), Disasters implied by Equity Index Options, *The Journal of The American Finance Association*, Vol. 66, No. 6, pp. 1969-2012;

[9] Bada, M. e Nurse, J.R.C., (2019), "The Social and Psychological Impact of Cyber-Attacks", *Emerging Cyber Threats and Cognitive Vulnerabilities*, pp.73-92;

[10] Baer, W. e Parkinson, A. (2007) Cyberinsurance in IT Security Management, *IEEE Security and Privacy Magazine*, Vol. 5, No. 3, pp. 50-56;

[11] Betterley, R.S., (2010), *Understanding the Cyber Risk Insurance and Remediation Services Marketplace. A Report on the Experiences and Opinions of Middle Market CFOs*, disponibile a http://betterley.com/samples/crmm_10_nt.pdf;

[12] Bichara, D., Iggidir, A. e Sallet G., (2013), Global analysis of multi-strains SIS, SIR and MSIR epidemic models, *Journal of Applied Mathematics and Computing*, Vol. 44, pp. 273-292;

[13] Bichara, D., Kang, Y., Castillo-Chavez, C., Horan, R. e Perrings, C., (2015), *SIS* and *SIR* epidemic models under virtual dispersal, *Bull Math Biol.*, Vol. 77, No. 11, pp. 2004-2034;

[14] Biener, C., Eling, M. e Hendrik Wirfs, J., (2014), Insurability of Cyber Risk. An Empirical Analysis, *The Geneva Papers on Risk and Insurance*, Vol. 40, pp. 131-158;

[15] Blackwell, D., (1953), Equivalent Comparisons of Experiments, *The Annals of Mathematical Statistics*, Vol. 24, No. 2, pp. 265-272;

[16] Bohme, R. e Kataria, G., (2006), *Models and measures for correlation in cyber-insurance*, Workshop on the Economics of Information Security, disponibile a https://www.econinfosec.org/archive/weis2006/docs/16.pdf;

[17] Bohme, R. e Schwartz, G., (2010), *Modeling cyber-insurance: Towards a unifying framework*, disponibile a http://www.icsi.berkeley.edu/pubs/networking/modelingcyber10.pdf;

[18] Cabrales, A., Gossner, O. e Serrano, R., (2013), Entropy and the Value of Information for Investors, *American Economic Review*, Vol. 103, No. 1, pp. 360-377;

[19] CISCO (2018), *2018 Cisco Annual Cybersecurity Report*, disponibile a https://www.cisco.com/c/dam/m/hu_hu/campaigns/security-hub/pdf/acr-2018.pdf;

[20] Clayton, D.G., (1978), A Model for Association in Bivariate Life Tables and Its Application in Epidemiological Studies of Familial Tendency in Chronic Disease Incidence, *Biometrika*, Vol. 6, No. 1, pp. 141-151;

[21] Compare, G., (2019), *Principi della sicurezza informatica. Become an Ethical Hacker*, indipentently published, s.l.;

[22] Coval, J., Jurek, J. e Stafford, E., (2009), Economic Catastrophe Bonds, *American Economic Review*, Vol. 99, No. 3, pp. 628-666;

[23] Craigen, D., Diakun-Thibault, N. e Purse, R., (2014), Defining Cybersecurity, *Technology Innovation Management Review*, Vol. 4, No. 10, pp. 13-21;

[24] CSIS (2018), *Rethinking Cybersecurity: Strategy. Mass Effect, and States*; disponibile a https://www.csis.org/analysis/rethinking-cybersecurity;

[25] CSIS (2018), *The Economic Impact of Cybercrime*; disponibile a https://www.csis.org/analysis/economic-impact-cybercrime;

[26] Debreu, G., (1977), *The Theory of Value. An Axiomatic Analysis of Economic Equilibrium*, Yale Univ Pr, s.l.;

[27] Durand, D., Iagolnitzer, Y., Krzanik, P., Loge, C., Susini, J., (2013), "Middleware for the Internet of Things: Principles", *RFID and the Internet of Things*, pp.183-215;

[28] Eling, M. e Schnell, W., (2016), What do we know about cyber risk and cyber risk insurance?, *The Journal of Risk Finance*, Vol. 17, No. 5, pp. 474-491;

[29] Embrechts, P., Lindskog, F. e Mcneil, A., (2003), Modelling Dependence with Copulas and Applications to Risk Management, *Handbook of Heavy Tailed Distributions in Finance*, Vol. 1, No. 8, pp. 329-384;

[30] Evans, A., (2019), *Managing Cyber Risk*, Routledge, s.l., 1. edizione;

[31] EY (2019), *Is cybersecurity about more than protection? EY Global Information Security Survey*, disponibile a https://assets.ey.com/content/dam/ey-sites/ey-com/en_ca/topics/advisory/ey-global-information-security-survey-2018-19.pdf;

[32] Frees, E.W. e Valdez, E., (1998), Understanding relationships using copulas, *North American Actuarial Journal*, Vol. 2, No. 8, pp. 1-25;

[33] Goddard, M., (2017), The EU General Data Protection Regulation (GDPR). European regulation that has a global impact, International Journal of Market Research, Vol.59, No. 6, pp. 703-705;

[34] Gold, J., (2017), Key Considerations for Cyberrisk Coverage, *Risk Management*, Vol. 64, No. 9;

[35] Gordon, L.A., Loeb, M.P. e Sohail, T., (2003), A framework for using insurance for cyber-risk management, *Communications of the ACM*, Vol. 46, No. 3, pp. 81-85;

[36] Guo, B. (2016), "Why Hackers Become Crackers – An Analysis of Conflicts Faced by Hackers", *Public Administration Research*, Vol. 5, No. 1;

[37] Gupta, A., (2019), *The IoT Hacker's Handbook. A practical Guide to Hacking the Internet of Things*, Apress, s.l., 1. edizione;

[38] Hasib, M., (2014), *Cybersecurity Leadership. Powering the Modern Organization*, CreateSpace Independent Publishing Platform, s.l., 3. edizione;

[39] Herath, H.S.B. e Herath, T.C., (2011), Copula-based actuarial model for pricing cyber-insurance policies, *Insurance Markets and Companies. Analyses and Actuarial Computations*, Vol. 2, No. 1, pp. 7-20;

[40] IBM (2019), *2018 Cost of Data Breach Study. Impact of Business Continuity Management*, disponibile a https://www.ibm.com/downloads/cas/AEJYBPWA;

[41] IBM Security (2019), *Cost of Data Breach Report 2019*, disponibile a https://www.allaboutsecurity.de/fileadmin/micropages/Fachartikel_28/2019_Cost_of_a_Data_Breach_Report_final.pdf;

[42] ICSAlabs (2005), *ICSA Labs 10th annual: Computer virus Prevalence Survey*, disponibile a https://www.yumpu.com/en/document/read/49262429/icsa-labs-10th-annual-virus-prevalence-survey-2004pdf-craig-/4;

[43] Investors, *American Economic Review*, Vol. 103, No. 1, pp. 360-377;

[44] ISACA (2019), *State of cybersecurity 2019: Current trends in attacks, awareness and governance*, disponibile a https://cybersecurity.isaca.org/csx-resources/state-of-cybersecurity-2019-part-2;

[45] Jang-Jaccard, J. e Nepal, S., (2014), A survey of emerging threats in cybersecurity, *Journal of Computer and System Sciences*, Vol. 80, No. 5, pp. 973-993;

[46] Kosub T. (2015) Components and challenges of integrated cyber risk management, *Zeitschrift für die gesamte Versicherungswissenschaft*, Vol. 104, pp. 615-634;

[47] Kruse, C.S., Frederick, B., Jacobson, T., Monticone, D.K., (2017), Cybersecurity in healthcare: A systematic review of modern threats and trends, *Technology and Health Care*, Vol. 25, No. 1, pp. 1-10;

[48] Kshetri, N., (2018), The Economics of Cyber-Insurance, *IT Professional*, Vol. 20, No. 6, pp. 9-14;

[49] Li, J. e Zou, X., (2009), Generalization of the Kermack-McKendrick SIR Model to a Patchy Environment for a Disease with Latency, *Mathematical Modelling of Natural Phenomena*, Vol. 4, No. 2, pp. 92-118;

[50] Majuca, R.P., Yurcik, W. e Kesan, J.P., (2006), *The Evolution of Cyberinsurance*, disponibile a https://arxiv.org/abs/cs/0601020;

[51] Mallik, A., Ahsan, A., Shahadat, M., Tsou, J.C., (2019), Man-in-the-middle-attack: Understanding in simple words, *International Journal of Data and Network Science*, Vol. 3, pp. 77-92;

[52] Maochao, X. e Lei, H., (2017), Cybersecurity Insurance: Modeling and Pricing, *North American Actuarial Journal*, Vol. 23, No. 2, pp. 220-249;

[53] MaryAnne, M. Gobble, (2013), Big Data: The Next Big Thing in Innovation, *Research-Technology Management*, Vol. 56, pp. 64-67;

[54] Moore, R. (2006), *Cybercrime. Investigating High-Technology Computer Crime*, Anderson, s.l., 2. edizione;

[55] Mukhopadhyay, A. Chatterjee, S., Saha, D., Mahanti A. e Sadhukhan, S.K., (2006), *E-Risk management with insurance: A framework using copula aided Bayesian belief networks*, lavoro presentato alla 39th Hawaii International International Conference on Systems Science, 4-7 January 2006, Kauai, HI, USA;

[56] Nelsen, R.B., (2006), *An introduction to Copulas*, Springer Verlag, s.l., 2. edizione;

[57] NetDiligence (2019), *Cyber claims Study 2019 report*, disponibile a https://netdiligence.com/2019-cyber-claims-study-landing/;

[58] Regolamento UE 2016/679, OJ L 119, 04.05.2016, cor. OJ L 127, 23.5.2018;

[59] Richardson, R. (2008), *2008 CSI Computer Crime & Security Survey. The latest results from the longest-running project of its kind*, disponibile a http://www.sis.pitt.edu/jjoshi/courses/IS2150/Fall11/CSIsurvey2008.pdf;

[60] Rinne, H., (2008), *The Weibull Distribution*, Chapman and Hall/CRC, s.l., 1. edizione;

[61] RISKIQ (2019), *Evil Internet in a Minute,* disponibile a https://www.riskiq.com/infographic/evil-internet-minute-2019/;

[62] Ryu, S. e Song, T.M., (2014), Big Data Analysis in Healthcare. Promise and potential, *Health Information Science and Systems,* Vol. 2, No. 3;

[63] Schwartz, G.A. e Sastry, S.S., (2014), *Cyber-insurance framework for large-scale interdependent networks*, lavoro presentato alla HiCoNS '14: 3rd International Conference on High Confidence Networked Systems, Berlin Germany, Aprile 2014;

[64] Schweizer, B, (1991), Thirty years of Copulas, *Advances in Probability Distributions with Given Marginals,* Vol.67, pp. 13-50;

[65] Selby, J., (2018), *Demystifying Cyber Insurance. For data breach and more: 5 Steps to the Right Coverage, s.l.*;

[66] Selby, J., (2019), *A Closer Look at Cyber Insurance. Exploring New Coverages, Including for GDPR and Other Regulations*, s.l.;

[67] Shannon, C. e Weaver, W., (1948), *Mathematical Theory of Communication*, Univ of Illinois Pr, s.l.;

[68] Singer, P.W. e Friedman, A., (2014), *Cybersecurity and cyberwar. What Everyone Needs to Know*, Oxford University Press, s.l., 1. edizione;

[69] Sklar, A., (1973), Random variables, joint distribution functions, and copulas, Kybernetika, Vol. 9, No. 6, pp. 449-460;

[70] Smith, M.S., (2011), *Bayesian Approaches to Copula Modelling*, disponibile a https://arxiv.org/abs/1112.4204;

[71] Stephen, M.W., (2019), *A quick cyber insurance guide for GDPR compliance*, disponibile a http://techgenix.com/cyber-insurance-guide/;

[72] Stoneburner, G., Goguen, A. e Feringa, A. (2002), *Risk Management Guide for Information Technology Systems*, disponibile a https://www.nist.gov/publications/risk-management-guide-information-technology-systems;

[73] Symantec (2019), *Internet Security Threat Report*, volume 24, disponibile a https://www.symantec.com/it/it/security-center/threat-report;

[74] Tankard, C., (2016), What the GDPR means for business, *Network Security*, Vol. 2016, No. 6, pp. 5-8;

[75] Taylor, H., (2018), Cyber SecurityIntroduction to Cybersecurity, *The missing report*, disponibile a https://preyproject.com/blog/en/what-is-cyber-security/;

[76] TrustArc (2019), *CCPA and GDPR Compliance ReportResearch into U.S. Compliance Status and Plans for California Consumer Privacy Act and EU General Data Protection Regulation*, disponibile a https://www.trustarc.com/blog/2019/04/17/ccpa-and-gdpr-compliance-report-new-research-measures-compliance-status-and-plans-for-ccpa-and-gdpr-part-3-of-3/;

[77] United States Census Bureau (2008), *Bureau of Justice Statistics Special Report. Cybercrime against Businesses 2005*, disponibile a https://www.bjs.gov/content/pub/pdf/cb05.pdf;

[78] United States Census Bureau (2019), *2020 Census. Safety and Security*, disponibile a https://www.census.gov/library/fact-sheets/2019/dec/2020-safety-security.html;

[79] Vade Secure (2019), *Phishers' favorites top 25*, Q1 2019, Worldwide Edition, disponibile a https://www.vadesecure.com/en/phishers-favorites-q1-2019/;

[80] Vegh, S., (2002), Hacktivists or Cyberterrorists? The Changing Media Discourse on Hacking, *First Monday*, Vol. 7, No. 10;

[81] Verizon (2019), *2019 Data Breach Investigations Report*, disponibile a https://enterprise.verizon.com/resources/reports/dbir/;

[82] Verlaine, M., (2020), *On the Extraction of Cyber Risks using Structured Products*, disponibile a https://ssrn.com/abstract=3509741;

[83] Voigt, P. e von dem Bussche, A., (2017), *The EU General Data Protection Regulation (GDPR). A practical guide*, Springer International Publishing, s.l., 1. edizione;

[84] von Solms, B. e von Solms, R., (2018), "Cybersecurity and information security – what goes where?", *Information and Computer Security*, Vol. 26, No. 1, pp. 2-9;

[85] Walker, B., (2019), *Cyber security: Comprehensive Beginners Guide to Learn the Basics and Effective Methods of Cyber Security*, independently published, s.l.;

[86] Yan, J., (2007), Enjoy the Joy of Copulas: With a Package copula, *Journal of Statistical Software. Foundation for Open Access Statistics*, Vol. 21, No. 4;

[87] Yang, Z. e Lui, J.C.S., (2014), Security adoption and influence of cyber-insurance markets in heterogeneous networks, *Performance Evaluation*, Vol. 74, pp. 1-17;

[88] Yeo, J. e van der Ende, R., (2019), *Advancing Cyber risk management. From security to resilience*, disponibile a https://www.oliverwyman.com/content/dam/marsh/Documents/PDF/US-en/advancing-cyber-risk-management-from-security-to-resilience.pdf;

[89] Zhan, Z., Xu, M. e Xu, S., (2015), Predicting Cyber Attack Rates with Extreme Values, *IEEE Transactions on Information Forensics and Security*, Vol. 10, No. 8, pp. 1666-1667;

SITOGRAFIA

[1] Agenda Digitale, https://www.agendadigitale.eu/;

[2] Avg, https://www.avg.com/it/signal/man-in-the-middle-attack;

[3] Cyber security 360, www.cybersecurity360.it;

[4] Global Rates, https://it.global-rates.com/tassi-di-interesse/euribor/2005.aspx;

[5] ICO, https://ico.org.uk/for-organisations/guide-to-data-protection/;

[6] IM Irwin Mitchell, https://www.irwinmitchell.com/business/regulatory-compliance/gdpr-data-protection;

[7] Insureon, https://www.insureon.com/insurance-glossary/cyber-liability-first-party;

[8] Lloyds Bank, https://resources.lloydsbank.com/insight/cyber/cyber-risk/;

[9] Norton, https://us.norton.com/internetsecurity-emerging-threats.html;

[10] Statista, https://www.statista.com/topics/2445/cyber-insurance/;