ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

SCUOLA DI INGEGNERIA E ARCHITETTURA

Dipartimento di Informatica – Scienza e Ingegneria

Corso di Laurea in Ingegneria Informatica

Analisi di significativi eventi di violazione di cybersicurezza e correlazione con le conseguenze finanziarie, incluso l'impatto sul mercato azionario

Relatore:
Prof. Dr. Marco Prandini

Presentata da:
Leonardo Ciacco

Appello unico
Anno Accademico 2024-2025

Ringraziamenti

Grazie

Indice

Elenco delle Figure

Elenco delle Tabelle

Capitolo 1

Introduzione

Introduzione

Capitolo 2

Analisi dello stato dell'arte e del contesto

Il presente capitolo mira a fornire le informazioni fondamentali, necessarie a comprendere i futuri sviluppi. A questo scopo sono definiti alcuni concetti chiave in ambito di sicurezza informatica:

- rischio
- sicurezza
- minaccia
- vulnerabilità
- attacco

Con **rischio** si intende la possibilità che azioni umane o eventi abbiano un impatto su ciò a cui è attribuito valore. È quindi corretto affermare che si tratta di una grandezza, e come tale è quantificabile, è infatti direttamente proporzionale alla probabilità di avvenimento e all'impatto che avrebbe sui beni colpiti. La valutazione del rischio, mirata alla sua gestione e controllo, parte dalla stima quanto più accurata di queste due variabili.

La **sicurezza** è il processo di contenimento del rischio che consiste essenzialmente nella cura di tre proprietà fondamentali: riservatezza (inaccessibilità delle informazioni a chi non ha il permesso di consultarle), integrità (garanzia di correttezza delle informazioni) e disponibilità(possibilità di accesso e utilizzo delle informazioni e i servizi offerti).

La **minaccia** consiste nella potenziale compromissione di una o più delle proprietà sopracitate, e, da concetto astratto, si concretizza in un **attacco**: azione di sfruttamento (*exploit*) delle vulnerabilità di un sistema

2.1 Tipologie di attacco

ENISA (Agenzia dell'Unione europea per la cybersicurezza) raggruppa gli attacchi informatici in otto categorie principali.[1]

2.1.1 Ransomware

Definito come un tipo d attacco in cui gli attori coinvolti prendono il controllo di un bene del bersaglio e chiedono un riscatto (in inglese *ransom*) in cambio della restituzione. È un tipo di attacco fatto generalmente per scopi economici, ma, essendo anche uno dei più diffusi evolve rapidamente, sia dal punto di vista delle tecniche di estorsione che degli obiettivi.

2.1.2 Malware

Si tratta di un termine ombrello, descrive tutti i software o firmware con lo scopo di eseguire un processo non autorizzato sulla macchina ospitante il cui risultato è la compromissione di una delle tre propietà della sicurezza.

2.1.3 Ingegneria sociale

Gli attacchi tramite ingegneria sociale si distinguono per lo sfruttamento della vulnerabilità derivata dall'errore umano. Consistono nel mettere in atto tecniche di manipolazione per indurre chi coinvolto nella gestione dei beni bersaglio a rilasciare informazioni sensibili, concedere permessi apparentemente innocui, visitare siti, aprire file, documenti o e-mails con contenuto malevolo. Un esempio può essere il *phishing*, attacco in cui si cerca di indurre la vittima ad aprire un link ad un sito che scarica un *malware*.
L'ingegneria sociale è spesso protagonista delle fasi iniziali di un attacco, ma questo non esclude che possa essere impiegata in stadi più avanzati. Ad esempio, è chiamata BEC (*Business E-mail Compromise*) l'intrusione tramite vecchie credenziali aziendali che le sfrutta, fingendosi parte dell'organizzazione, per ottenere dagli ex colleghi informazioni, denaro, o risorse altrimenti inaccessibili.[2]

2.1.4 Violazioni di dati

Tecnicamente vi ci si riferisce con i termini inglesi *data breach* o *data leak*. Da definizione del GDPR, per violazione dei dati personali intendiamo la "violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati" (articolo 4.12 GDPR).
La differenza risiede nell'intenzionalità: il *breach* è un attacco con l'esplicito obiettivo di ottenere o diffondere dati sensibili o protetti, il *leak* è originato da un errore che porta ad una indesiderata perdita o messa a disposizione di dati sensibili.

2.1.5 Minacce alla disponibilità: DoS

Per definizione, un DDoS (*Distriubuted Denial of Service*), si verifica come risultato di un attacco che mira a rendere inaccessibili servizi o risorse tramite, per esempio, uno sproporzionato volume di richieste che sovraccarica i componenti della struttura attaccata. In questo caso quindi l'obiettivo risiede nella semplice interruzione dei servizi erogati.

2.1.6 Minacce alla disponibilità: minacce ad Internet

Alla base della disponibilità dei servizi nella società dell'informazione vi è l'infrastruttura di internet, che se subisce guasti distribuiti può comprometterne quasi completamente l'erogazione. Sebbene sia un'ipotesi remota, blackout, disastri naturali, interruzione forzata da parte del governo o attacchi su larga scala rappresentano una minaccia concreta che non può essere sottovalutata.

2.1.7 Manipolazione delle informazioni

Si chiama *Foreign Information Manipulation and Interference*, abbreviato in FIMI, l'insieme di strategie di manipolazione dell'opinione pubblica da parte di enti, governativi e non, volte ad inserirsi nel dibattito in maniera massiccia e organizzata. Ciò mina i processi decisionali democratici tramite campagne di disinformazione e narrazioni precostruite.

2.1.8 Attacchi alla catena di fornitura

Più comunemente chiamati *supply chain attacks*, sono attacchi che sfruttano la fiducia riposta nei servizi offerti da partner commerciali o fornitori, colpendo l'obiettivo indirettamente tramite la compromissione di un fornito-

re legittimo.
Più formalmente, un attacco è considerato in parte di natura *supply chain* se consiste nella combinazione di almeno due attacchi coordinati. Perché sia identificato come tale, devono infatti essere bersaglio sia l'obiettivo intermedio, fornitore, che l'obiettivo finale, naturalmente vulnerabile nei confronti chi valuta fonte sicura.

2.2 Contesto economico

Con l'esponenziale crescita ed espansione dei mezzi di informazione, crescono anche i mercati illeciti, precisamente il costo del cybercrimine era di $3 trilioni nel 2015 e, si stima, toccherà i $10.5 trilioni durante il 2025[3]. Se fosse il PIL di uno stato sarebbe sicuramente tra i primi cinque al mondo.
In un panorama di questo tipo le aziende quotate in borsa, soprattutto le più in risalto come quelle in indici come S&P500, sono un bersaglio estremamente appetibile per chiunque abbia i mezzi e l'intenzione di danneggiarle in quanto:

- sono in possesso di grandi quantità di **dati sensibili**: questo sopratutto se si tratta di grandi aziende o se specializzate nel settore, ma chiaramente, se l'obiettivo è il furto di informazioni, un'alta concentrazione delle stesse agisce da incentivo;
- sono facilmente **valutabili**: per eseguire un attacco *ransomware* occorre anche commisurare la richiesta di riscatto al valore del bene per l'azienda e alla sua disponibilità economica, i bilanci pubblici offrono quindi una fonte di informazioni preziosa;
- se attaccate, hanno **reazioni** spesso **prevedibili**: secondo un rapporto di Accenture del 2010 [4], le aziende che subiscono un attacco sperimentano un calo di prezzo delle azioni che si aggira solitamente intorno al 5%, rivelando come l'attacco potrebbe essere sfruttato ulteriormen-

te come strumento di controllo illecito del mercato per trarre ulteriori profitti collaterali.

Solo nel 2023, il 21% selle aziende in S&P500 hanno subito un *breach*[5].
Inoltre, i danni connessi agli attacchi sono ugualmente preoccupanti, tra questi:

- ripercussioni legali;
- perdita di fiducia di clienti ed investitori.

Un attacco può avere diversi scopi, di cui, primo tra tutti, quello economico, ma il panorama degli attacchi è vasto, e pensare di non poter essere bersagli appetibili è un errore pericoloso per l'azienda e chiunque vi sia collegato. [1]
A fronte di ciò risulta già evidente quanto sia necessario essere a conoscenza dell'entità del rischio di un attacco informatico che, vista anche la forte crescita e diffusione, non può essere ignorata. Va quindi sviluppato un piano d'azione dettagliato e coerente con la valutazione dei beni a rischio, finanziato adeguatamente.

2.3 Metodologia

Lo studio si propone di analizzare 15 casi di attacchi informatici, con focus sulle ripercussioni che questi hanno avuto sull'azienda.
Gli attacchi sono di vario tipo, e sono avvenuti tra il 2011 e il 2024 l'analisi è condotta con l'obiettivo di individuare un trend e ,in generale, valutare la minaccia crescente del cybercrimine.

Capitolo 3

Attacchi e conseguenze finanziarie

Nota: la maggior parte dei grafici proviene da macrotrends.

3.1 Sony Playstation Network (2011)

3.1.1 Descrizione

Il 20 aprile 2011 Sony dichiarò che tra il 17 e il 19 dello stesso mese avvenne un importante *data breach* , a seguito di cui disabilitò per una settimana il servizio online Playstation Network. L'attacco portò al furto di dati sensibili riguardanti 77 milioni di account[6][7].

3.1.2 Impatto diretto

Sony subì diverse conseguenze legali, che unite agli obblighi di miglioramento della sicurezza, si stima ebbero un costo complessivo di $171 milioni.

3.1.3 Impatto indiretto

Come si puòvedere dalla figura 3.1 e nelle fonti [7] la compagnia subì, nei primi giorni, un calo del valore delle azioni ben superiore al 3%.

Figura 3.1: Impatto a breve termine Sony Playstation Network Outage

A seguito inizia un periodo di contrazione che, possiamo osservare, porta i valori delle azioni da più di $5 nel periodo antecedente alla crisi, fino a scendere sotto i $2 nel 2013 (adjusted).
Associare la parabola discendente esclusivamente all'attacco è forse esagerato, ciò non toglie che si tratti sicuramente di un fattore rilevante.

Figura 3.2: Impatto a lungo termine Sony Playstation Network Outage

3.1.4 Note

Le comunicazioni furono tardive e poco precise, gli azionisti ebbero notizia del motivo per cui Playstation Network era disabilitato solo 7 giorni dopo, e i comunicati ai clienti non furono da meno, alimentando malcontento e sfiducia nelle capacità dell'azienda[7].

3.2 Target (2013)

3.2.1 Descrizione

Il caso di *data breach* affrontato riguarda l'azienda di distribuzione Target, seconda, negli Stati Uniti, solamente a Walmart, e l'attacco che si è concluso con il furto di informazioni, comprese informazioni di pagamento e carte di credito, di 70 milioni di clienti.
Prime avvisaglie dell'ingresso di un malware nella rete arrivano il 30 novembre 2013, probabilmente avvenuto per via dell'utilizzo di passwords troppo semplici nei server aziendali, ma è dal 12 dicembre che, in seguito alla notifi-

ca del Dipartimento di Giustizia, iniziano le indagini congiunte. Verificatane l'entità, la notizia viene resa di dominio pubblico il 19 dicembre 2013[8].

3.2.2 Impatto diretto

Da quanto dichiarato nei bilanci SEC (*Securities and Exchange Commission*), le spese dirette, tolti $90 milioni coperti da assicurazione, ammontano a $200 milioni[8].

3.2.3 Impatto indiretto

Sebbene nei giorni immediatamente successivi ci sia stato un picco verso il basso di -2.2% 3.3, con momenti di ulteriore discesa, e sebbene la crescita sia stata praticamente neutra per un anno, dalla fine del 2014 l'azienda ha recuperato parte della crescita inespressa fino ad allora 3.4. Ad aiutare è stata l'ottima immagine che ha nei confronti dei clienti e la fiducia dei più affezionati ad un marchio decisamente forte.

Figura 3.3: Impatto a breve termine Target data breach

Figura 3.4: Impatto a lungo termine Target data breach

3.3 Sony Pictures (2014)

3.3.1 Descrizione

Sony Pictures Entertainment viene colpito da un attacco informatico di tipo *data breach* a fine novembre 2014, vengono rilasciati 40GB di informazioni che, a detta degli attaccanti, fanno parte di un furto del volume di 100TB. Dentro vi troviamo più di 6800 dati salariali dei dipendenti, e anticipazioni riguardanti serie TV e film ancora in fase di produzione[9].

3.3.2 Impatto diretto

L'azienda dichiara, nel bilancio SEC per aziende estere, di aver speso $41 milioni per spese investigative e correlate all'attacco e che dovrà sostenere spese legali nei confronti di dipendenti ed ex dipendenti[10]. A fine anno troverà un accordo per stanziare $8 milioni di risarcimento.

3.3.3 Impatto indiretto

Come notiamo in figura 3.5, l'attacco ha progressivamente portato le azioni dell'intero gruppo Sony a -5% e fino a toccare il -10% a metà dicembre, sopratutto per l'importante risonanza mediatica del caso e il fatto che fosse la seconda volta in pochi anni che il nome della compagnia era accostato a casi di furto di informazioni.

Figura 3.5: Impatto a breve termine Sony Picture hack

Sul lungo periodo l'andamento si è probabilmente svincolato dalla discesa iniziale, anche grazie alla diffusa gamma di attività in di cui si occupa il gruppo 3.6. L'impatto quindi non è quantificabile in maniera semplice, ma è ragionevole pensare che il danno di immagine si sia protratto a lungo.

Figura 3.6: Impatto a lungo termine Sony Picture hack

3.3.4 Note

La copertura dei media e la grande mole di notizie riguardanti il caso derivano dall'associazione dell'attacco alla Corea del Nord e ad un film in uscita, prodotto da SPE, "The Interview", in cui la storia sarebbe stata costruita attorno al tentato assassinio del leader Kim Jong Un. Nella gestione della crisi, l'essere protagonisti di un evento tanto discusso ha sicuramente contribuito ad aggravare i danni d'immagine connessi alla vicenda[9].

3.4 Yahoo (2013, 2014)

3.4.1 Descrizione

A settembre 2016 rende noto che nel 2014 sono stati rubati i dati personali di 500 milioni di utenti a seguito di un attacco di ingegneria sociale[11]. Il 14 dicembre 2016 Yahoo comunica che, mentre investigava al riguardo, ha scoperto un secondo furto: durante agosto 2013 è avvenuto quello che ricor-

diamo come il più grande *data breach* della storia. Inizialmente venne dichiarato si trattasse di 1 miliardo, poi, nel 2017 il dato si assesterà solidamente sui 3 miliardi di account di cui sono state diffuse informazioni[11][12].

3.4.2 Impatto diretto

L'azienda era in fase di acquisizione da parte di Verizon che, ritrattando il prezzo a ribasso, passò da un'offerta di $4,83 miliardi ad un prezzo finale, nel 2017, di $4,48 determinando una perdita effettiva di $350 milioni[11]. Inoltre i procedimenti portarono l'azienda a pagare altri $35 milioni per un patteggiamento con la SEC e $117 milioni per risarcire gli utenti colpiti.

3.4.3 Impatto indiretto

Nel breve termine possiamo osservare una discesa di quasi il 10% da settembre alla fine di dicembre 2016 prima di una crescita che anticipa l'acquisizione.

Figura 3.7: Impatto a breve termine Yahoo data breach

Nel periodo prossimo all'acquisto di Yahoo, Verizon subisce un calo del 6%. Osservare oltre l'andamento rischia di essere fuorviante per via dei diver-

si componenti dell'azienda al tempo, ma le azioni seguono un trend in crescita

Figura 3.8: Impatto a lungo termine Verizon (Yahoo) data breach

3.4.4 Note

1. la fonte dei grafici storici di yahoo è https://companiesmarketcap.com/, in quanto non è stato possibile procurarsi dati più precisi di una azienda il cui ticker non esiste più;

2. la gestione delle comunicazioni da parte dell'azienda è stata tardiva a dir poco, contribuendo ad aggravare la posizione dell'azienda nei confronti dell'opinione pubblica e della legge.

3.5 Uber (2016, 2022)

3.5.1 2016

Descrizione

Il *data breach* avvenne ad ottobre 2016, ma la divulgazione risale a ben un anno dopo, grazie ad un cambio di dirigenza. I rischi che ha corso nel gestire ambiguamente il caso hanno rischiato di avere conseguenze penali[13].

Impatto diretto

L'azienda, oltre al riscatto pagato agli hacker per eliminare i dati rubati, ha concordato coi 50 stati americani il pagamento di una multa di $148 milioni.

Impatto indiretto

Al tempo l'azienda non era quotata, quindi non è possibile analizzare questo aspetto, se non osservando il caso del 2022.

Note

Una aggravante è stata sicuramente la gestione consapevolmente ingannevole, per esempio rivelò l'esistenza del *breach* a SoftBank, permettendo poi che comprasse una buona parte della compagnia a prezzo ribassato[13].

3.5.2 2022

Descrizione

Tramite ingegneria sociale l'attaccante è riuscito ad entrare nel sistema di condivisione di informazioni aziendali Slack, con conseguente arresto forzato di alcuni servizi da parte dell'azienda il 13 settembre 2022[14].

Impatto diretto

La prontezza della reazione ha permesso di contenere le conseguenze dirette dell'attacco, evitando eventuali sanzioni.

Impatto indiretto

Il mercato ha invece reagito più bruscamente di quanto visto fin'ora 3.9, con un picco verso il basso di -10% rispetto al giorno della scoperta (ancor più pronunciato se prendiamo in esame il 15 settembre, data della dichiarazione). Ad un mese di distanza la discesa rallenta ma non si arresta.

Figura 3.9: Impatto a breve termine Uber 2022

Per tornare in pari ci vogliono più di sette mesi, indice che i precedenti attacchi avevano lasciato un segno importante nella reputazione dell'azienda.

Figura 3.10: Impatto a lungo termine Uber 2022

Note

Il primo data breach e le sue conseguenze sono servite a Uber per cambiare approccio alla sicurezza e migliorato diversi aspetti[14].

3.6 FedEx - NotPetya (2017)

3.6.1 Descrizione

Il *ransomware* NotPetya fu un attacco diffuso su larga scala, con epicentro in Ucraina, a giugno del 2017.Sua peculiarità era di non essere stato concepito per scopi di lucro, quanto più invece per causare disordine e distruzione[15], secondo un rapporto della Casa Bianca i danni ammontarono complessivamente a $10 miliardi[16].
In questo contesto, l'azienda FedEx Corporation, che aveva da poco fatto acquisizioni in Europa (TNT Express), affrontò grossi disservizi nel vecchio continente che complicarono i processi di assimilazione[17].

3.6.2 Impatto diretto

Nel bilancio depositato a SEC si stimano le perdite intorno ai $400 milioni che rallentarono la crescita durante il primo quarto dell'anno fiscale (giugno-agosto 2017).

3.6.3 Impatto indiretto

Essendo l'azienda distribuita, e in forte crescita negli Stati Uniti, l'impatto distruttivo di NotPetya non è roboante come ci si aspetterebbe da uno dei più costosi attacchi della storia. Di fatti, dal 27 giugno 2017 (giorno dell'attacco) le azioni crescono ed iniziano una discesa solo qualche tempo

dopo, scendendo fino a -5%.

Figura 3.11: Impatto a breve termine NotPetya su FedEx

Come già discusso ci sono segnali di una ripresa abbastanza forte, che in mancanza dell'attacco, sarebbero potuti essere lo specchio di una crescita importante.

Figura 3.12: Impatto a lungo termine NotPetya su FedEx

3.6.4 Note

La diffusione così ampia di un attacco lo assimila, agli occhi dell'opinione pubblica, ad un disastro naturale o comunque ad un fattore esterno, intaccando più tramite costi diretti che indiretti le aziende coinvolte. I danni di immagine risultano quindi significativamente contenuti.

3.7 Equifax (2017)

3.7.1 Descrizione

L'8 settembre 2017, l'agenzia di informazioni creditizie al consumo americana Equifax rilascia un comunicato in cui dichiara che ha subito un *data breach* che interessa 148 milioni di cittadini statunitensi. L'attacco è stato possibile grazie al mancato aggiornamento tempestivo di alcuni server con una specifica vulnerabilità nota, presente dell'URL[18].

3.7.2 Impatto diretto

Come conseguenza della grande quantità di cause indette contro Equifax, l'azienda arrivò a concordare un impegno monetario di $575-$700 milioni[19].

3.7.3 Impatto indiretto

L'impatto fu molto pesante, a distanza di tre giorni osserviamo un calo dell' 8,20%, che va oltre il 20% a metà settembre. Questo è dovuto ad una massiccia vendita delle azioni, pari a $1,8 milioni[13]

Figura 3.13: Impatto a breve termine Equifax breach

Sul lungo periodo l'azienda fatica a risollevarsi, complici le pesanti sanzioni e la perdita di fiducia degli investitori.

Figura 3.14: Impatto a lungo termine Equifax breach

3.7.4 Note

Pare che il fatto fosse noto alla dirigenza già da inizio agosto 2017[13] è stata, insieme al tipo di informazioni perse, una pesante aggravante in ambito legale.

3.8 British Airways (2018)

3.8.1 Descrizione

Il *data breach*, attuato tramite l'iniezione di 22 linee di codice Javascript malevolo via URL (*cross site scripting*, XSS), che colpì la compagnia aerea del Regno Unito, British Airways, venne reso pubblico il 6 settembre 2018 da un comunicato pubblico del *National CyberSecurity Centre*. Le vittime, le cui stime iniziali ne dichiaravano 380 000, si scoprono ad ottobre essere ben 565 000, di cui sono trapelati nomi, email e informazioni delle carte di credito.[20]

3.8.2 Impatto diretto

L'azienda ha sostenuto una multa di $20 milioni come conseguenza dell'attacco. [20] La pena ridotta è probabilmente una concessione dovuta alla successiva crisi causata dal COVID-19.

3.8.3 Impatto indiretto

La compagnia è nel gruppo *International Airlines Group* e quotata nelle borse inglesi e spagnole, pertanto discuteremo l'andamento di quest'ultimo tramite i dati ufficiali di *London Stock Exchange*.
Il gruppo, come evidenziato nelle fonti[20] ha una perdita quasi immediata del 2%, e continua a scendere durante tutto il mese successivo.

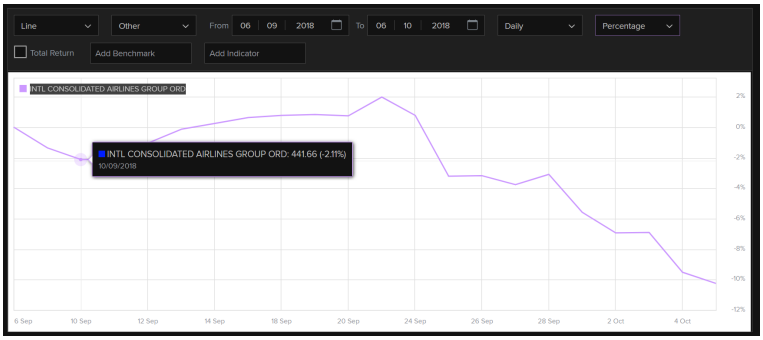


Figura 3.15: Impatto a breve termine British Airways

Nel lungo periodo le azioni risentono del danno di immagine fino all'inizio del 2020, in cui però, la compagnia ha ricadute legate all'inizio della pandemia del COVID-19.

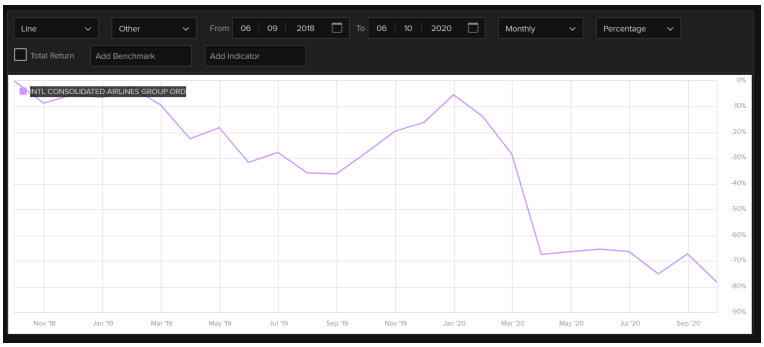


Figura 3.16: Impatto a lungo termine British Airways

3.9 Marriot International (2018)

3.9.1 Descrizione

L'attacco si distribuisce su un ampio lasso di tempo: nel 2014, tramite accesso fisico ad un terminale con permessi di amministratore, viene installato un *malware* nella rete di Starwood, agenzia alberghiera statunitense. Dopo aver trovato la chiave di decrittazione dei database e aver esfiltrato i dati, gli attaccanti cifrarono nuovamente le informazioni per non lasciare tracce. Così fu anche dopo l'acquisizione di Starwood da parte di Marriott International nel 2016, tanto da passare inosservata fino all'8 settembre 2018. Seguirono investigazioni che culminarono nella dichiarazione del 30 novembre 2018, in cui si rivelava la diffusione di informazioni di approssimativamente 500 milioni di clienti in tutto il mondo[21][22].

3.9.2 Impatto diretto

Come spese di riparazione interne Marriott dichiara $30 milioni [21], in aggiunta pagò anche una multa di £18,4 milioni al Regno Unito [23], sebbene inizialmente le cifre dichiarate fossero intorno ai £99 milioni.

3.9.3 Impatto indiretto

Il giorno dell'annuncio registra un calo di più del 5% arrivando oltre -17% sotto Natale. Marriott dichiarò una perdita stimata di $1 miliardo dovuta alla perdita di fiducia dei clienti[21].

Figura 3.17: Impatto a breve termine Marriott International data breach

Negli anni successivi torna a crescere fino ad inizio 2020, anche qui, si suppone dovuta alla contrazione del mercato di quel periodo.

Figura 3.18: Impatto a lungo termine Marriott International data breach

3.9.4 Note

La crisi è stata generata da errori nel controllo dei sistemi informativi e della rete dell'a società acquisita, evidenziando come l'espansione di un'azienda in tal modo sia fonte di vulnerabilità talvolta inaspettate. Per quanto l'azienda abbia provato a scaricare la responsabilità dell'accaduto altrove, risulta evidente come questo sia un compito cruciale da svolgere durante grandi o piccole operazioni di fusione.

3.10 Capital One (2019)

3.10.1 Descrizione

La holding bancaria Capital One Financial Corporation scopre, tramite una mail proveniente da un esterno di un *data breach* che ha interessato 100 milioni di cittadini statunitensi e 6 milioni canadesi, pubblicherà quindi un comunicato al riguardo il 29 luglio 2019[24].

3.10.2 Impatto diretto

Oltre alla multa di $80 milioni, ha poi raggiunto un accordo di risarcimento dal valore di $190 milioni ad inizio 2022 [25].

3.10.3 Impatto indiretto

Come è osservabile in figura 3.19, al giorno del comunicato è seguito un crollo di quasi il 6% e le azioni hanno continuato la discesa per tutto il mese successivo.

Figura 3.19: Impatto a breve termine Capital One

Ormai è evidente il trend di ripresa (in questo caso moderata) e crollo ad inizio 2020, qui presente anche se la holding non è direttamente connessa a settori turistici, a evidenziare la pervasività della crisi finanziaria seguita al Covid-19.

Figura 3.20: Impatto a lungo termine Capital One

3.10.4 Note

Anche se molte fonti non individuano in Capital One errori grossolani, il percepito e la risposta del mercato sono stati netti.

3.11 SolarWinds (2020)

3.11.1 Descrizione

L'azienda di sviluppo di software aziendale SolarWinds è stata coinvolta, nel corso del 2020, in un *supply chain attack* che l'ha vista protagonista della distribuzione di *malware*.
A febbraio 2020, dopo aver ottenuto l'accesso alla rete aziendale, viene iniettato codice malevolo all'interno del prodotto Orion contenente una *backdoor*, questi, che avrebbe poi assunto il nome di SUNBURST, venne distribuito in un aggiornamento software a partire da marzo, sfruttando i certificati che garantivano l'autenticità della sorgente per rimanere occultato. Seguirono

attacchi mirati fino all'8 dicembre 2020, in cui l'agenzia di cybersicurezza FireEye non si accorse del furto di alcuni suoi strumenti, portando poi alla rivelazione al pubblico in data 13 dicembre 2020.
L'attacco colpì tra i 17 000 e i 18 000 clienti di SolarWinds, compresi enti governativi [26][27][28].

3.11.2 Impatto diretto

Stime riportano il costo per le compagnie assicurative di $90 milioni. SolarWinds in particolare ha poi concordato con la SEC una sanzione di $26 milioni [29].

3.11.3 Impatto indiretto

Possiamo vedere la portata distruttiva che ha avuto l'attacco sulle azioni, con una discesa pari a -34,66% in un solo mese, e l'inizio di un trend discendente che è durato più di un anno.

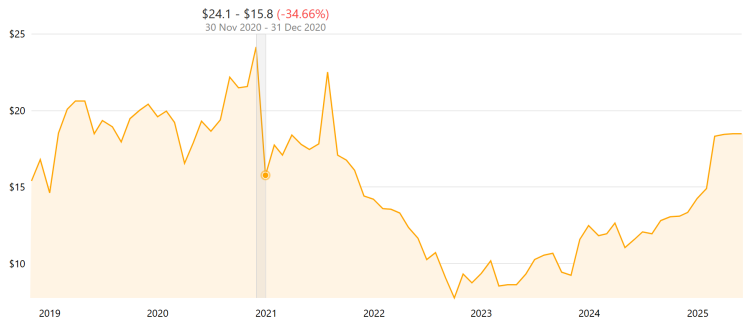


Figura 3.21: Impatto SolarWinds supply chain attack

3.11.4 Note

La compagnia è stata acquistata nella pima metà del 2025, perciò i dati provengono nuovamente da https://companiesmarketcap.com/

3.12 Colonial Pipeline (2021)

3.12.1 Descrizione

L'attacco *ransomware* alla compagnia di trasporto di carburanti è stato compiuto tramite BEC (tipo particolare di ingegneria sociale) con lo scopo di ottenere un riscatto di $4,4 milioni in BitCoin.
Ricevuta la richiesta di riscatto, il 7 maggio 2021, la dirigenza di Colonial Pipeline decise di arrestare l'imipianto e pagare gli attaccanti nel tentativo li limitare i danni [30].

3.12.2 Impatto diretto

Il riscatto, sebbene sia stata recuperata una parte ($2,3 milioni) rimane un costo affrontato dall'azienda [30].

3.12.3 Impatto indiretto

Nonostante l'azienda non ha subito riduzioni di prezzo delle azioni, non essendo quotata, la comunità ha sofferto la mancanza improvvisa del servizio, con aumenti esponenziali di prezzo e reazioni di panico generale [31].

3.13 MGM Resorts (2023)

3.13.1 Descrizione

Dal 10 settembre 2023 iniziano a trapelare indiscrezioni rigiuardo a comunicazioni tra l'FBI, il *Nevada Gaming Control Board* e l'azienda multinazionale di intrattenimento, gioco d'azzardo e ospitalità MGM Resorts, a

seguito di cui, l'11 settembre, verrà rilasciato un comunicato in cui si annuncia l'arresto di alcuni servizi e l'inizio di indagini in merito ad un attacco informatico.
La natura del *ransomware attack* diviene presto nota grazie alla rivendicazione da parte del gruppo di hacker ALPHV/BlackCat, che si è intrusa nel sistema tramite ingegneria sociale via telefonica (*vishing*).
Nonostante la risposta pronta e la collaborazione stretta con le autorità, sono state rubate informazioni riguardanti clienti e dipendenti, compromettendo la posizione di MGM Resorts International di fronte alla legge in materia di protezione dei dati personali [32].

3.13.2 Impatto diretto

MGM Resorts dichiara meno di $10 milioni in spese di consulenza legale, coperti in larga parte da assicurazione [33]. Ha in corso alcuni procedimenti , e ha patteggiato per un fondo di risarcimento per il caso del 2023 e uno precedente, del 2019, di $45 milioni [34].

3.13.3 Impatto indiretto

Nel rapporto straordinario a SEC si stima una perdita di $100 milioni nell'Adjusted Property EBITDAR (indicatore del fatturato ante tasse, interessi, ammortamenti, deprezzamenti e spese di affitto aggiustato per escludere spese straordinarie).
Come si nota in figura 3.22, rispetto alle performances pre annuncio del *data breach* e l'arresto dei servizi, viene registrato un calo superiore al 5%, che tocca un picco di -20% a inizio ottobre.

Figura 3.22: Impatto a breve termine MGM Resorts

Come da rapporto, era prevista una ripresa grazie ad un evento di Formula 1 [33], ma il calo successivo può essere connesso al danno di immagine subito.

Figura 3.23: Impatto a lungo termine MGM Resorts

3.13.4 Note

L'attacco è ben documentato anche grazie ad un rapporto pubblicato dagli attaccanti stessi che, per alcuni, pare vogliano così presentarsi come una controparte ragionevole nelle trattative che si sviluppano attorno ai loro attacchi *ransomware*.

3.14 Change Healthcare (2024)

3.14.1 Descrizione

Change Healthcare Inc. è un gestore di pagamenti nel circuito sanitario statunitense parte della holding United Healthcare Group. Il 21 febbraio 2024 denuncia l'ingresso non autorizzato nei suoi sistemi da parte del, già menzionato, gruppo di hacker *ransomware* BlackCat. Per limitare i danni ha istantaneamente disattivato tutti i servizi, creando uno scompenso nel sistema sanitario nazionale. Nonostante tutto è stato stimato che siano trapelate le informazioni di 192,7 milioni di persone [35] [36].

3.14.2 Impatto diretto

Nel tentativo di recuperare i dati rubati, Change Healthcare, ha pagato $22 milioni,a questo punto però, il gruppo BlackCat si ritirò dalle trattative con il riscatto, e l'intermediario che le aveva gestite, ancora in possesso dei dati, ne chiese un secondo, che non fu corrisposto [35]. A questo si aggiungeranno le spese legali dei processi in corso.
Come impatti diretti, in un report sul terzo quarto dell'anno fiscale 2024, viene stimato a $1,521 miliardi il costo diretto per United Health.

3.14.3 Impatto indiretto

Essenndo UH un gruppo ampio, e che le ripercussioni dell'attacco sono arrivate prima ad aziende più piccole, con limitata capacità di gestire la crisi, è plausibile che il grafico non riporti una discesa istantanea, ma un picco verso il basso che parte quasi una settimana dopo l'annuncio del *breach*.
La perdita nel breve termine si assesta comunque tra il 10% e il 5%.

Figura 3.24: Impatto a breve termine Change Healthcare

Dopo luglio 2024 l'azienda ha iniziato il recupero, ma ad oggi pare in una crisi ancora peggiore di cui le sanzioni in arrivo, le perdite, gli ingenti prestiti fatti ($9,7 miliardi [36]) e il danno di immagine non sono protagonisti, ma hanno sicuramente un ruolo.

Figura 3.25: Impatto a lungo termine Change Healthcare

Capitolo 4

Analisi dei dati aggregati

Raccolgo in una tabella le analisi che si possono fare riguardo ai casi presentati, usando l'EBITDA degli anni fiscali degli attacchi per mettere in prospettiva i costi diretti (per le aziende quotate).

Nome soggetto colpito	**Anno**	**Tipo di attacco**	**Costo diretto in milioni di$ (c.d. / EBITDA)**	**Effetto sulle azioni**
Sony Playstation Network	2011	data breach	171 (14,82% [37])	-3% – -5%
Target	2013	data breach	200 (2,84% [38])	-2,2%
Sony Pictures	2014	data breach	49 (1,22% [10])	-5% – -10%
Yahoo	2014	data breach	152 (11,16% [39])	-9,54%
Uber	2016	data breach	148	–
Uber	2022	ingegneria sociale	0	-10% – -15%
FedEx	2017	ransomware (NotPetya)	400 (5,02% [17])	-5,03%
Equifax	2017	data breach	circa 625 (56,2% [40])	-8,2% – -20%
British Airways	2018	data breach via XSS	26 (0,48% [41])	-2%
Marriott International	2018	data breach via phisical malware injection	53,92 (2,05% [42])	-5% – -17%
Capital One	2019	data breach	270 (1,75% [43])	-5,89% – -12%
SolarWinds	2020	supply chain	26 (5,3% [44])	-34,66%
Colonial Pipeline	2021	ransomware	2,1	–
MGM Resorts	2023	ransomware via vishing	32,5+ (0,7+% [45])	-5,2% – -20,5%
Change Healthcare	2024	ransomware, data breach	1 521 (4,2% [46])	-5% – -10%

Tabella 4.1: Tabella comparativa

4.1 Note

- la maggior parte degli ebitda che non sono esplicitati nei report in quanto non è obbligatorio a fini fiscali, sono spesso ottenuti tramite la formula $EBITDA = OperatingIncome + Depreciacion\&Amortisation$

- Sony nel 2012 ha un, con cambio valuta del periodo, registra un EBITDA di $1,154 miliardi

- l'EBITDA di Sony nel 2014vale $4,032 miliardi

- nel caso del data breach di Yahoo non viene considerato il deprezzamento di 350 milioni nei costi

- le multe in sterline applicate a Marriott International e British Airways dal Regno Unito sono convertite con un tasso di cambio di 1,3 (£ to $) del 2018

- per capital one, ho ricavato e utilizzato il valore di EBITDA per coerenza con il resto dello studio pur non essendo il un indicatore spesso usato per banche. Nello specifico ho aggiunto al *net income* le tasse, il costo degli interessi, deprezzamento e ammortamento

- il costo del processo a MGM Resorts è dimezzato per tenere in considerazione il fatto che la multa sia legata anche ad un altro caso

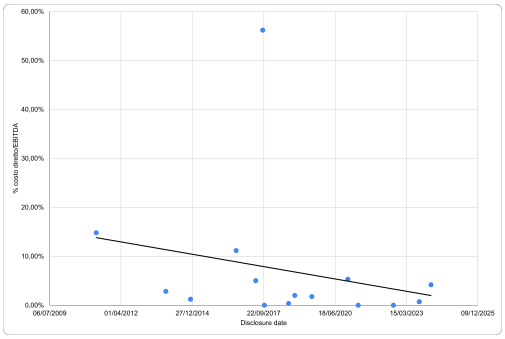
- dal rapporto di United Health, per evincere l'EBITDA si è utilizzata la formula $EBITDA = Earnings + Amortisation$

Possiamo notare come le premesse iniziali riguardanti un calo dele azioni del 5% siano state rispettate in larga parte [4].

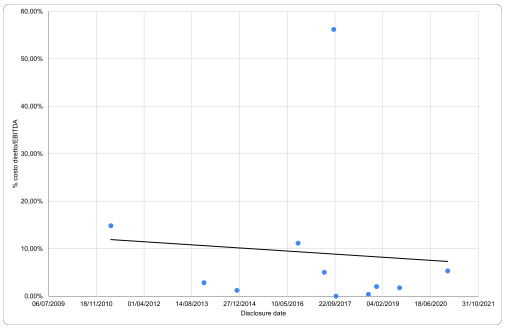
4.2 Dati linearizzati

4.2.1 EBITDA

Come si può notare da figura 4.1a e figura 4.1b si evidenzia un trend in calo. La prima è sicuramente condizionata dal fatto che alcuni dei processi di MGM Resorts e Change Healthcare sono ancora in corso, e sono quindi incompleti. Ciò viene corretto nel secondo grafico, ottenendo una linearizzazione che denuncia un calo meno pronunciato.



(a) EBITDA nel tempo



(b) EBITDA nel tempo corretto

Il trend discendente evidenzia un calo dei costi diretti in relazione alla redditività dell'azienda, che potrebbe derivare da una maggiore prontezza ed efficienza nella gestione sul piano tecnico da parte delle aziende di media-grande dimensione prese in esame nello studio.

4.2.2 Azioni

Quanto detto prima non si applica al percepito e alla reazione dei mercati finanziari secondo figura 4.2. Il trend crescente funge da monito e restituisce un quadro in cui la prevenzione rimane centrale nonostante il calo di costi diretti connessi agli attacchi.

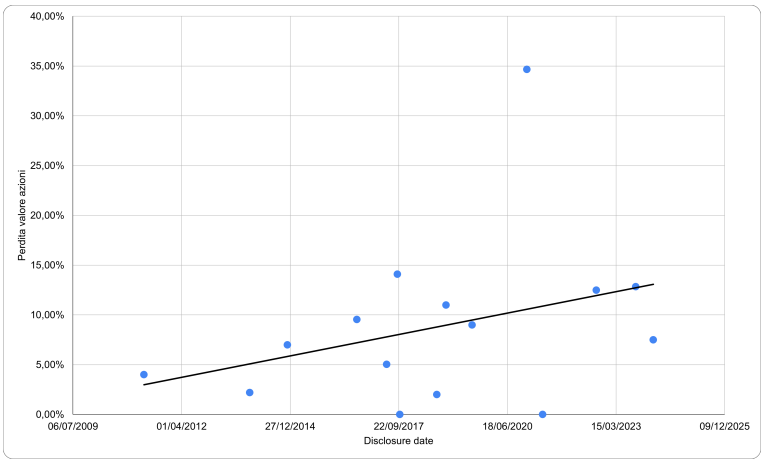


Figura 4.2: Perdita di valore delle azioni a breve termine nel tempo

Capitolo 5

Conclusioni

Lo studio evidenzia una controtendenza rispetto all'effettiva crescita del costo degli attacchi informatici menzionata precedentemente e una crescente propensione a crolli considerevoli nel valore di mercato e l'incremento nel tempo del numero di attacchi *ransomware*, sebbene una valutazione su un campione così ridotto sia esposta ad errori.
È possibile interpretare questo dato come una minore propensione o minore efficacia degli hacker negli attacchi a grandi aziende che si dimostrano sempre più preparate. Ma se comunque il costo complessivo è in fortissima crescita [3] il risultato è un danno maggiore per enti collegati o un aumento del numero assoluto di attacchi ad aziende più piccole che spesso non si interessano sufficientemente o non hanno i mezzi adeguati.
A fronte di ciò risulta evidentemente necessario potenziare per qualunque azienda la propria copertura in ambito di sicurezza informatica. In italia, dove la maggioranza delle aziende sono piccole o medie imprese, sarebbero probabilmente efficaci degli incentivi statali che, aiutando lo sviluppo di un livello adeguato di protezione in maniera capillare, permetterebbe di ridurre considerevolmente anche i danni agli enti connessi.

Bibliografia

[1] European Union Agency for Cybersecurity, I. Lella, C. Ciobanu, E. Tsekmezoglou, M. Theocharidou, E. Magonara, A. Malatras, and R. Svetozarov Naydenov, *ENISA threat landscape 2023 - July 2022 to June 2023*, I. Lella, C. Ciobanu, E. Tsekmezoglou, M. Theocharidou, E. Magonara, A. Malatras, and R. Svetozarov Naydenov, Eds. ENISA, 2023. [Online]. Available: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

[2] IBM. Cos' è la compromissione dell'e-mail aziendale (BEC)? IBM. [Online]. Available: https://www.ibm.com/it-it/topics/business-email-compromise

[3] S. Morgan. (2020, Nov.) Cybercrime to cost the world $10.5 trillion annually by 2025. Cybersecurity Ventures. Editor-in-Chief: Steve Morgan. [Online]. Available: https://cybersecurityventures.com/annual-cybercrime-report-2016/

[4] "How global organizations approach the challenge of protecting personal data," Accenture and Ponemon Institute LLC, Report, 2010. [Online]. Available: https://www.ponemon.org/local/upload/file/ATC_DPP%20report_FINAL.pdf

[5] P. Prudhomme. The cybersecurity of the S&P 500: An in-depth analysis from securityscorecard. SecurityScorecard. Blog post. [Online]. Available: https://securityscorecard.com/blog/the-cybersecurity-of-the-sp-500/

[6] B. Quinn and C. Arthur. (2011, Apr.) Playstation network hackers access data of 77 million users. The Guardian. [Online]. Available: https://www.theguardian.com/technology/2011/apr/26/playstation-network-hackers-data

[7] E. U. Jørgensen, "The stakeholder attributions of corporate crisis responsibility following a cyber attack," 2018.

[8] M. Plachkinova and C. Maurer, "Teaching case: Security breach at target," *Journal of Information Systems Education*, vol. 29, no. 1, pp. 11–20, winter 2018.

[9] BuzzFeed News. (2015, Mar.) A look through the sony pictures data hack. Exhibit 2002 in CBM2015-00030, PTAB. [Online]. Available: https://www.docketalarm.com/cases/PTAB/CBM2015-00030/Covered_Business_Method_Patent_Review_of_U.S._Pat._6321201/03-10-2015-Patent_Owner/Exhibit-2002-Exhibit_2002___A_Look_Through_The_Sony_Pictures_Data_Hack___BuzzFeed_News/

[10] Sony Corporation, "Form 20-f: Annual report pursuant to section 13 or 15(d) of the securities exchange act of 1934 for the fiscal year ended march 31, 2015," U.S. Securities and Exchange Commission, Annual Report, 2015. [Online]. Available: https://www.sec.gov/Archives/edgar/data/313838/000119312515231346/d895998d20f.htm

[11] N. Daswani and M. Elbayadi, *The Yahoo Breaches of 2013 and 2014*. Berkeley, CA: Apress, 2021, pp. 155–169. [Online]. Available: https://doi.org/10.1007/978-1-4842-6655-7_7

[12] S. Thielman. (2016, Dec.) Yahoo hack: 1bn accounts compromised by biggest data breach in history. [Online]. Available: https://www.theguardian.com/technology/2016/dec/14/yahoo-hack-security-of-one-billion-accounts-breached

[13] J. M. Robbins and A. M. Sechooler, "Once more unto the breach: What the equifax and uber data breaches reveal about the intersection of information security and the enforcement of securities laws," *Criminal Justice*, vol. 33, no. 1, pp. 4–7, spring 2018.

[14] K. Joonas, A. Y. Mahfouz, A. Banks, D. Murphy, T. Johnson, J. Napper, and L. Luellin, "Data breach in the service sector: Problems and solutions," in *Proceedings of the Twenty-Second AIMS International Conference on Management*. AIMS International, 2022.

[15] U. K. A. Bangalore Ghousekhan, "The evolution of ransomware: A case study of wannacry and notpetya," *ResearchGate*, vol. 4, pp. 2009–2014, 11 2017.

[16] A. Greenberg. (2018, Aug.) The untold story of notpetya, the most devastating cyberattack in history. [Online]. Available: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world

[17] FedEx Corporation, "Form 10-k: Annual report pursuant to section 13 or 15(d) of the securities exchange act of 1934, for the fiscal year ended may 31, 2018," U.S. Securities and Exchange Commission, Annual Report, 2018. [Online]. Available: https://www.sec.gov/Archives/edgar/data/1048911/000156459018016877/fdx-10k_20180531.htm

[18] J. Thomas, "A case study analysis of the equifax data breach 1 a case study analysis of the equifax data breach," *ResearchGate*, 12 2019.

[19] Federal Trade Commission. (2019, Jul.) Equifax to pay $575 million as part of settlement with ftc, cfpb, and states related to 2017 data breach. [Online]. Available: https://www.ftc.gov/news-events/news/press-releases/2019/07/equifax-pay-575-million-part-settlement-ftc-cfpb-states-related-2017-data-breach

[20] M. Aljaidi, "A comprehensive technical analysis of url redirect attacks: A case study of british airways data breach," in *2023 24th International Arab Conference on Information Technology (ACIT)*, 2023, pp. 1–5.

[21] R. Denuwan, "Marriott international data breach," *ReserchGate*, 07 2023.

[22] J. E. Park, A. Reed, and A. Fan. (2023) Who's the real victim? marriott's victimization and customers' perception of it - marriott data breach crisis in 2018. Working Paper, SSRN. [Online]. Available: https://ssrn.com/abstract=4921991

[23] GDPR Register. (2020, Oct.) Ico fines marriott international inc £18.4 million for failing to keep customers' personal data secure. [Online]. Available: https://www.gdprregister.eu/news/ico-fine-marriot/

[24] N. Novaes Neto, S. E. Madnick, A. Moraes G. de Paula, and N. Malara Borges. (2020, Mar.) A case study of the capital one data breach. Working Paper; 25 pages; Posted: 17 Mar 2020. [Online]. Available: https://ssrn.com/abstract=3542567

[25] S. K. Gainey and T. C. Taylor. (2022) Capital one reaches $190 million settlement in connection with 2019 data breach. Moore & Van Allen. Articolo di blog di uno studio legale specializzato. [Online]. Available: https://www.mvalaw.com/data-points/capital-one-reaches-190-million-settlement-in-connection-with

[26] M. Marelli, "The solarwinds hack: Lessons for international humanitarian organizations," *International Review of the Red Cross*, vol. 104, no. 919, p. 1267–1284, 2022.

[27] I. S. Bala, A. Ebere, O. Junior, and Y. Filibus, "Cyberwarfare and arms control: Analyzing the solarwinds hack of 2020," *International Journal of Emerging Multidiciplinaries Social Science*, vol. Vol 3, 11 2024.

[28] R. Alkhadra, J. Abuzaid, M. AlShammari, and N. Mohammad, "Solar winds hack: In-depth analysis and countermeasures," in *2021 12th International Conference on Computing Communication and Networking Technologies (ICCCNT)*, 2021, pp. 1–7.

[29] SolarWinds Corporation. (2022) Form 10-Q for the quarterly period ended October 28, 2022. [Online]. Available: https://www.sec.gov/ix?doc=/Archives/edgar/data/1739942/000173994222000091/swi-20221028.htm

[30] J. Beerman, D. Berent, Z. Falter, and S. Bhunia, "A review of colonial pipeline ransomware attack," in *2023 IEEE/ACM 23rd International Symposium on Cluster, Cloud and Internet Computing Workshops (CCGridW)*, 2023, pp. 8–15.

[31] R. Dudley and D. Golden. (2021, May) The colonial pipeline ransomware hackers had a secret weapon: Self-promoting cybersecurity firms. Co-published with MIT Technology Review. [Online]. Available: https://www.propublica.org/article/the-colonial-pipeline-ransomware-hackers-had-a-secret-weapon-self-promoting-cybersecurity

[32] S. Schappert. (2023, ottobre) Titans in crisis: unraveling the mgm and caesars ransomware timeline. Consultato il 21 agosto 2025. [Online]. Available: https://cybernews.com/security/mgm-caesars-ransomware-attack-timeline

[33] MGM Resorts International, "Form 8-K: Current Report," Securities and Exchange Commission (SEC), Tech. Rep., Oct. 2023. [Online]. Available: https://www.sec.gov/Archives/edgar/data/789570/000119312523251667/d461062d8k.htm

[34] MGM Resorts International Data Breach Settlement. Official website for the class action settlement. [Online]. Available: https://www.mgmdatasettlement.com/

[35] HIPAA Journal. (2025, Aug.) Change Healthcare Increases Ransomware Victim Count to 192.7 Million Individuals. [Online]. Available: https://www.hipaajournal.com/change-healthcare-responding-to-cyberattack/

[36] A. Fliegelman and D. Stemp, "The cyberattack on change healthcare: Lessons for financial stability," Office of Financial Research, U.S. Department of the Treasury, Tech. Rep. OFR Brief 24-05, Nov. 2024. [Online]. Available: https://www.financialresearch.gov/briefs/files/OFRBrief-24-05-change-healthcare-cyberattack.pdf

[37] Sony Corporation, "Amendment no. 1 on form 20-f/a for the three months ended june 30, 2012 (english translation of the quarterly securities report)," Securities and Exchange Commission (SEC), Tech. Rep., July 2012, amendment No. 1 on Form 20-F/A; English translation of Japanese Quarterly Securities Report (Shihanki Hokokusho). [Online]. Available: https://www.sec.gov/Archives/edgar/data/313838/000119312512284981/d305818d20f.htm

[38] Target Corporation, "Form 10-k, annual report pursuant to section 13 or 15(d) of the securities exchange act of 1934, for the fiscal year ended february 2, 2013," Securities and Exchange Commission (SEC), Tech. Rep., 2013. [Online]. Available: https://www.sec.gov/Archives/edgar/data/27419/000104746913003100/a2213506z10-k.htm

[39] Yahoo! Inc., "Form 10-k, annual report pursuant to section 13 or 15(d) of the securities exchange act of 1934, for the fiscal year ended december 31, 2014," Securities and Exchange Commission (SEC), Tech. Rep., 2014. [Online]. Available: https://www.sec.gov/Archives/edgar/data/1011006/000119312515066560/d826131d10k.htm

[40] Equifax Inc., "Annual report on form 10-k for the fiscal year ended december 31, 2017," Securities and Exchange Commission (SEC), Tech. Rep., 2017. [Online]. Available: https://www.sec.gov/Archives/edgar/data/33185/000033185180000011/efx10k20171231.htm

[41] International Airlines Group (IAG), "Annual financial report 2019 (in english)," IAG, Tech. Rep., 2019. [Online]. Available: https://www.iairgroup.com/media/uxjb1c0e/iag-cnmv-annual-finanical-report-2019-en.pdf

[42] Marriott International, Inc., "Annual report on form 10-k for the fiscal year ended december 31, 2018," Securities and Exchange Commission (SEC), Tech. Rep., 2018. [Online]. Available: https://www.sec.gov/Archives/edgar/data/1048286/000162828019002337/mar-q42018x10k.htm

[43] Capital One Financial Corporation, "Annual report on form 10-k for the fiscal year ended december 31, 2019," Securities and Exchange Commission (SEC), Tech. Rep., 2019. [Online]. Available: https://www.sec.gov/Archives/edgar/data/927628/000092762820000102/cof-12312019x10k.htm

[44] SolarWinds Corporation, "Annual report on form 10-k for the fiscal year ended december 31, 2020," Securities and Exchange Commission (SEC), Tech. Rep., 2020. [Online]. Available: https://www.sec.gov/Archives/edgar/data/1739942/000173994221000043/swi-20201231.htm

[45] MGM Resorts International, "Annual report on form 10-k for the fiscal year ended december 31, 2023," Securities and Exchange Commission (SEC), Tech. Rep., 2023. [Online]. Available: https://www.sec.gov/Archives/edgar/data/789570/000078957024000005/mgm-20231231.htm

[46] UnitedHealth Group Incorporated, "Annual report on form 10-k for the fiscal year ended december 31, 2024," Securities and Exchange Commission (SEC), Tech. Rep., 2024. [Online]. Available: https://www.sec.gov/Archives/edgar/data/731766/000073176625000063/unh-20241231.htm