L’impatto del cyber risk sul mercato finanziario

Case Studies


BY NC ND

Data pubblicazione: marzo 2020

1. EXECUTIVE SUMMARY

Il presente studio è volto alla comprensione degli effetti di un attacco cyber sul valore azionario di un'azienda. L'analisi si basa sulla metodologia "Event Study". I dati presi in considerazione sono storici su casi realmente avvenuti e di cui si ha avuto pubblicazione dell'evento stesso. Sono 60 i casi presi in

considerazione, su 221 totali analizzati, in quanto i sessanta sono di aziende quotate.
La finestra temporale presa in considerazione va da 10 giorni prima della pubblicazione dell'evento da parte dell'azienda a due giorni post pubblicazione.
La tipologia di attacco considerato varia dalla esfiltrazione di dati al blocco di dati tramite cifratura.
L'impatto medio sul valore azionario è attestato a circa il 7%, ma è un impatto limitato nel tempo e non è considerabile di lungo periodo. Pertanto, è anche difficile poterne approfittare con azioni speculative se non si è a conoscenza anticipatamente dell'evento stesso e della sua pubblicazione.

2. LA RILEVANZA DEL CYBER RISK

La gestione dei rischi è imprescindibile nell'attività delle istituzioni finanziarie come nelle aziende in generale.
L'Ente di Vigilanza bancaria della BCE che conduce l'esercizio di individuazione e valutazione dei rischi su base annua, in stretta collaborazione con le autorità nazionali competenti (ANC) e con il contributo dei gruppi di vigilanza congiunti (GVC), ogni anno stila i risultati salienti dell'esercizio di valutazione dei rischi, che riporta poi lungo le dimensioni della probabilità e dell'impatto i principali fattori dannosi per il sistema bancario dell'area dell'euro in un orizzonte di due o tre anni.

Secondo l'ultimo Report, pubblicato all'inizio del 2019, i tre fattori di rischio più importanti sono i seguenti: incertezze geopolitiche, consistenze dei crediti deteriorati (non-performing loans, NPL) e loro possibile accumulo in futuro, cyber crime e disfunzioni dei sistemi informatici.
A questi si aggiungono la rivalutazione del rischio nei mercati finanziari, il contesto caratterizzato da bassi tassi di interesse, la reazione delle banche alla normativa.

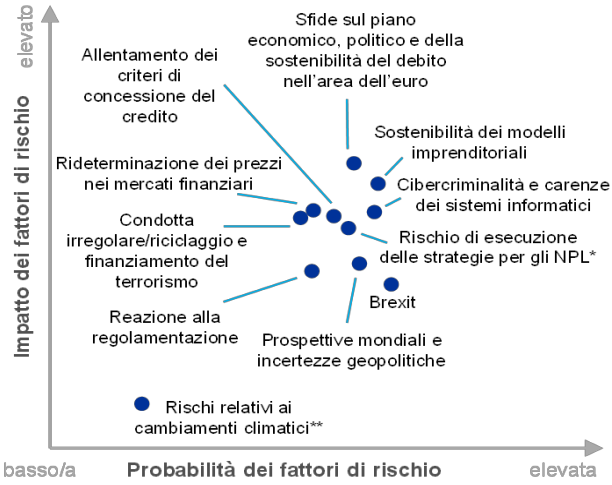

Figura 1: Fattori e probabilità di Rischio BCE e ANC

La rilevanza del rischio informatico c.d. Cyber Risk, è generata dalla crescente quantità di dati aziendali relativi non solo

all'attività di impresa svolta dai vari enti, ma anche di dati sensibili relativi a singoli individui che circolano all'interno del cyberspace e che hanno trasformato questa entità astratta e intangibile in un vero e proprio tesoro di informazioni esposte a interessi speculativi, politici o personali.
Le minacce sfruttano delle vulnerabilità o delle carenze nei sistemi causando delle conseguenze sistematiche sugli asset, sui processi o sui servizi, nonché danni reputazionali. Al fine di minimizzare le perdite, snellire le proprie strutture e perseverare verso l'efficienza, gli investimenti delle imprese nel rafforzamento della sicurezza informatica sono in costante aumento.
L'incremento del valore azionario di aziende che forniscono servizi di Cyber Security ne è la prova. Un esempio è l'azienda Check Point Software Technologies, una società di Tel Aviv che negli ultimi 5 anni ha registrato un incremento del valore azionario dell'80% e un incremento degli utili del 41%.

Il legame tra il valore azionario e gli attacchi informatici è ben noto e oggetto di accesi dibattiti. Infatti, il nesso tra gli eventi che colpiscono le aziende e le oscillazioni del valore delle securities [1] sul mercato finanziario ha ispirato l'approfondimento di metodi di analisi tecnica che potesse

[1] Locuzione inglese che indica il valore mobiliare in generale. Nel gergo finanziario viene impiegato nel senso più ristretto di azione o obbligazione

consentire di battere il mercato, cioè prevedere le oscillazioni dei prezzi dei titoli al fine di guadagnare così un rendimento molto elevato minimizzando i fattori di rischio.
Si agisce attraverso delle tecniche attive di investimento basate sul timing.
Per poter riuscire in un tale intento, le tempistiche e la quantificazione del danno rappresentano degli elementi imprescindibili nonché ostacoli che rendono l'impresa complessa persino per un insider.
A costituire il valore di una security non è solo l'impresa, ma il mercato stesso e come qualunque mercato si rispetti, vige la legge della domanda e dell'offerta, tale per cui, se improvvisamente iniziassero delle vendite massive di un titolo, il prezzo dello stesso diminuirebbe improvvisamente e questo annullerebbe qualunque beneficio nel breve periodo.
È necessario quindi comprendere quale sia il momento adatto per effettuare delle operazioni di "sell or buy" in base alla portata dell'evento che ha colpito l'azienda.
La cyber security nasce appositamente per attenuare le perdite derivanti dal cyber-risk. Le perdite di dati, dal punto di vista aziendale, sono strettamente connesse alle perdite di tipo economico, dunque, l'incremento di sistemi di protezione, permetterebbe la riduzione dell'impatto anche finanziario del rischio informatico.

Basata sui tre pilastri Risorse, Processi e Tecnologia, la disciplina è in costante sviluppo e intenta nel ricercare metodi di difesa sempre più efficaci in un sistema in continua evoluzione. Le minacce cyber sono in continua evoluzione e rappresentano uno degli elementi contro cui l'azienda deve predisporre misure efficaci onde evitare ingenti danni.

Gli attacchi informatici tendono ad incrementare di anno in anno. Il rapporto Clusit 2019 afferma che il numero degli attacchi informatici gravi siano aumentati del 37,7% dal biennio 2017-2018.

3. OBIETTIVO DELLO STUDIO E METODOLOGIA

Si intende presentare un'analisi focalizzata sull'impatto del cyber risk sui mercati finanziari, presentando dapprima le tipologie di minacce che corrono aziende e istituzioni per poi proiettarle sui mercati azionari attraverso la metodologia di analisi "Event Study" che registra l'impatto dell'informazione sull'andamento delle securities.

Il campione di riferimento è di tipo parziale. Una peculiarità di questo settore è relativa all'annuncio di aver subito un attacco informatico. Per motivi legati alla reputazione, a fattori legati alla "difficile individuazione", o a motivi sanzionatori, molti eventi vengono resi pubblici in ritardo o non vengono mai divulgati.

Nonché spesso la quantificazione è dubbia o non fornita. Dunque, nel campione selezionato, sono presenti solo quegli eventi che sono stati resi di pubblico dominio in via ufficiale e con una quantificazione ufficiale delle perdite superiore ad un milione di dollari. Gli eventi, che non hanno rispettato questi criteri, non sono stati inclusi nel campione per non incorrere nel rischio di contaminazione dei risultati.

Il campione, preso in considerazione, conta 221 aziende/enti/istituzioni finanziarie colpite da attacchi informatici rilevanti tra il 2011 e il 2019 appartenenti a quattro regioni geografiche differenti:

- NORAM (Canada, Stati Uniti e Messico);
- EMEA (Europa, Medio Oriente e Africa del Nord);
- JAPAC (Asia Pacifica, Giappone, Cina);
- LATAM (America Latina).

Di queste, quelle utilizzate per l'analisi Event Study sono state 60, in quanto quotate.

4. CYBER RISK

L'incremento della complessità del cyber space, ha fatto sì che incrementassero anche i rischi di potenziali attacchi.
Il rischio (R) è una funzione dipendente da 3 fattori: minaccia (M), vulnerabilità (V) e impatto (I).

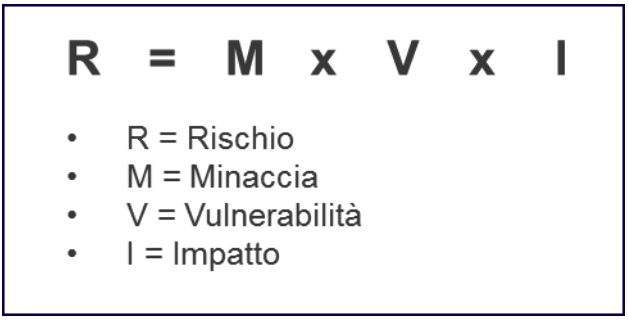

Figura 2: Formula del rischio

Il rischio dipende dunque dal fatto che una minaccia riesca a sfruttare una vulnerabilità di un sistema per causare un impatto o danno.
In questo studio, si considerano solo attacchi informatici come genere di minaccia. Non si contemplano errori umani o catastrofi naturali.
Gli attaccanti cercano di colpire i sistemi sfruttando delle vulnerabilità note o non note dei sistemi stessi. Il sistema viene visto come un insieme di servizi, interdipendenti, la cui

erogazione dipende da processi, risorse umane e beni materiali e immateriali.

La suddivisione delle minacce cibernetiche è effettuata a seconda delle finalità che gli attori perseguono. È possibile individuare quattro macro-categorie:

- **Cybercrime**: complesso delle attività con finalità criminali come la truffa o la frode telematica, il furto d'identità, la sottrazione di informazioni o di creazioni e proprietà intellettuali, in sintesi tutte le attività criminali commesse all'interno del cyber space che hanno uno scopo di lucro illecito;
- **Hacktivism**: perseguimento di obiettivi sociali e politici attraverso la pirateria informatica, termine derivante dall'unione delle parole "hacking" e "activism";
- **Espionage**: acquisizione indebita di dati/informazioni sensibili, proprietarie o classificate;
- **Cyber Warfare**: insieme delle attività e delle operazioni militari cibernetiche pianificate e condotte allo scopo di conseguire effetti in tale contesto.

Nello studio non verranno trattate le tecniche di attacco o le vulnerabilità sfruttate. Tantomeno verrà trattato il danno riportato dalle aziende.

Su quest'ultimo punto sono in corso molte discussioni nel settore dell'Information Security per arrivare ad una metodologia riconosciuta generalmente per valutare quantitativamente il danno.
Le metodologie quantitative, relative all'impatto del cyber crime, considerano principalmente perdite dirette e indirette causate dall'evento. Queste perdite vengono calcolate sulla base dei minori ricavi raggiunti, dei costi diretti e indiretti sostenuti per superare l'evento e per recuperare il danno reputazionale subito.
In questo caso, verrà osservato invece solo il variare del valore azionario, in uno specifico arco temporale di breve periodo, per comprendere se un attacco informatico, oltre agli impatti già considerati possa far fluttuare il valore del titolo azionario dell'azienda vittima.
Sulla base delle osservazioni condotte, lo studio vuole rispondere semplicemente alla seguente domanda: un attacco cyber andato a buon fine influisce sul valore azionario dell'azienda?

4.1. STATISTICHE ATTACCHI IDENTIFICATI

I settori colpiti maggiormente da criminalità informatica, risultano essere, in base al campione, il settore pubblico (23%) e quello finanziario (20%). Da sempre, questi sono nel mirino di

hacker e criminali informatici, in particolare, sono i settori maggiormente colpiti da attacchi di tipo “Hacktvism” e “Cyber-warfare”.
Un esempio ne sono i numerosi attacchi che hanno interessato Citigroup, Bank of America, PNC, Wells Fargo, JP Morgan e molte altre istituzioni finanziarie statunitensi da parte di “Izz ad-Din al-Qassam”, i cosiddetti Cyber Fighters, un gruppo estremista che nel 2013 rivendicava idee religiose.
Inoltre, l’obiettivo di gruppi di Hacktivist o Cyber-terrorist non è quasi mai l’obiettivo di guadagni illeciti, infatti tendono a pianificare attacchi come il DDoS (Distributed Denial of Service) che ha lo scopo di rendere un servizio o un’infrastruttura indisponibile sfruttando come fonti di attacco più sistemi informatici compromessi; oppure, si servono di attacchi di tipo APT (Advanced Persistent Threat), che, mirati e persistenti, rendono i sistemi vulnerabili e facilmente accessibili. Appartiene al cyber attivismo anche l’attività di Defacement, ovvero l’intrusione non autorizzata nel sito web con modifica dei contenuti del sito.
All’interno del campione analizzato, è possibile osservare come si distribuiscano le varie tipologie di attacco a seconda dell’area geografica.
Sugli attacchi analizzati:

- **75** per la regione NORAM;

- **62** per EMEA;
- **43** per JAPAC;
- **36** LATAM.

Il più diffuso risulta essere proprio l'attivismo informatico, mentre il Cyber-Warfare, risulta maggiormente concentrato nella regione del Medioriente (in EMEA) e negli Stati Uniti (in NORAM).
Un esempio è l'attacco del 10 settembre 2019, soprannominato "Foil Cyber-warfare", individuato nel Golfo Persico.
La figura seguente riporta il grafico a torta con i settori colpiti da attacchi informatici mentre a seguire ci sono
i grafici di distribuzione per le singole aree geografiche.

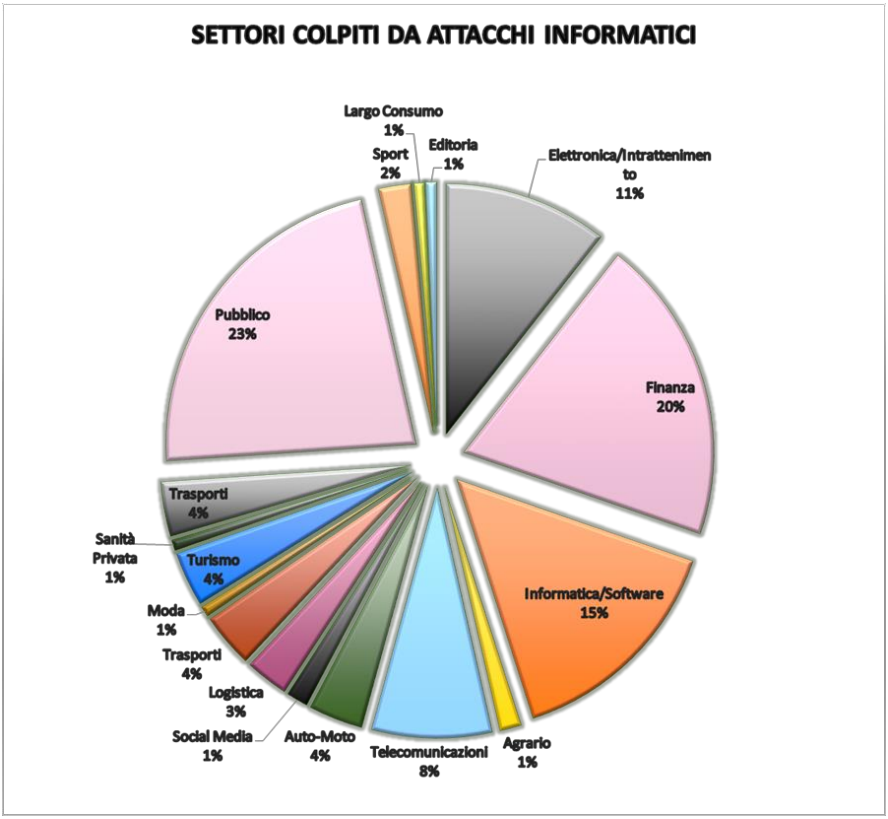

Figura 3: Distribuzione percentuale degli attacchi per settore

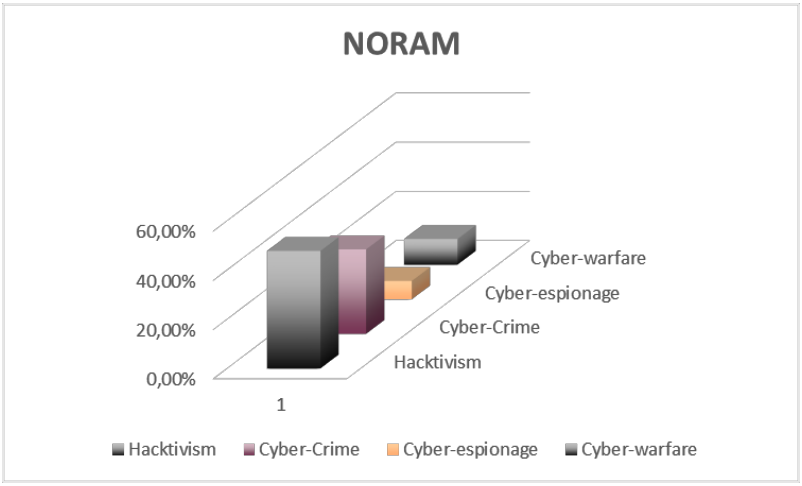

Figura 4: NORAM Distribuzione attacchi

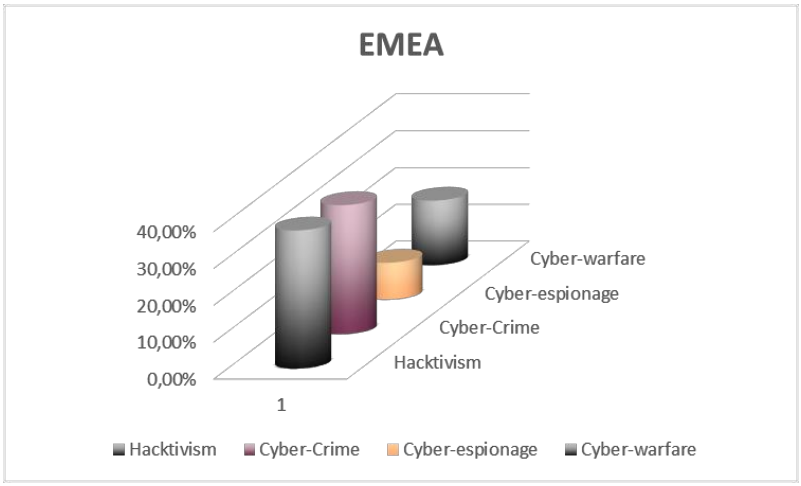

Figura 5: EMEA Distribuzione attacchi

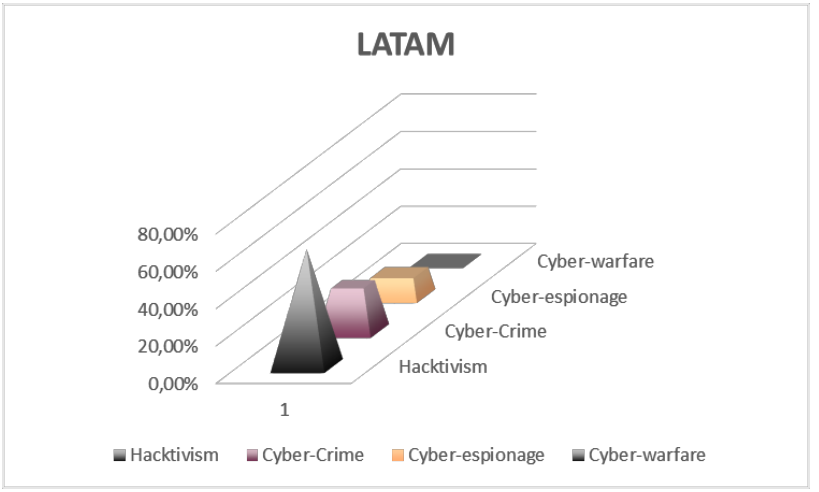

Figura 6: LATAM Distribuzione attacchi

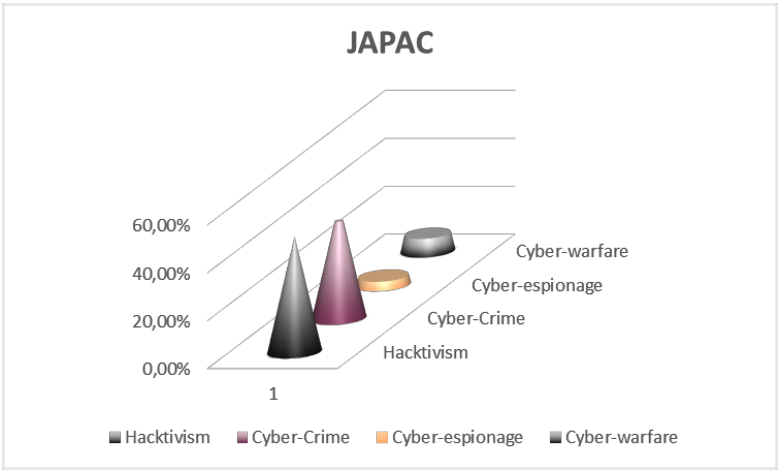

Figura 7: JAPAC Distribuzione attacchi

5. PRINCIPALI TECNICHE DI ATTACCO

Gli strumenti di cui dispongono i criminali informatici sono in continua evoluzione. In questa sede, solo a titolo esemplificativo, sono riportati quelli più diffusi.
Nella seguente Tabella:

Minaccia	Descrizione
Virus	Malware che una volta attivato è in grado di replicarsi e infettare sistemi operativi, file e singoli documenti.

Worm	Malware che è in grado di replicarsi e infettare tutti i sistemi connessi sulla stessa rete
Phishing o Spear-Phishing	Mail che sembrano provenire da soggetti conosciuti, ma che hanno l'intenzione di sottrarre password o dati di tipo finanziario
Attacco Brute-Force	Attacco capace di rubare password grazie ad un sistema che permette di generare diverse combinazioni alfanumeriche possibili in velocità
Cross-Site Scripting (XSS)	Attacco che sfruttando una vulnerabilità dei siti Web, che consente all'attaccante di iniettare degli script malevoli con l'intenzione di rubare informazioni riservate o installare malware sui browser degli utenti
SQL Injection	Tecnica di code injection, usata per attaccare applicazioni di gestione dati, con la quale vengono inserite delle stringhe di codice SQL malevole all'interno di campi di input in modo che vengano eseguiti
Vulnerabilità 0 Day	Vulnerabilità di applicazioni non ancora divulgate o per la quale non è stata distribuita una patch
Key Logger	Intercettazione in forma nascosta delle digitazioni
DDos	Attacco mirato a rendere indisponibile il sistema
Spam	Comunicazioni indesiderate al fine di diffondere Malware

APT	Attacco di difficile identificazione che ha l'obiettivo di generare punti di accesso ad una rete per lunghi periodi di tempo
Botnet	Rete di dispositivi infettati da malware e controllati da remoto per effettuare attività malevole
Poisoning	Hanno l'obiettivo di inquinare i contenuti presenti all'interno delle social network
Man in the Middle	Alterazione della comunicazione tra due parti con l'obiettivo di intercettarne i dati. Es: spoofing
Credit Card Record	Registrazione attraverso ATM o trasferimenti online di pagamenti e relativi dati finanziari
Defacement	Alterazione dei contenuti di un sito internet o di una piattaforma al fine di creare contenuti forvianti
Ransomware	Tipo di malware che blocca l'accesso al dispositivo chiedendo un riscatto al fine di ripristinare le normali funzioni.

Figura 8: Esempio tipologie di attacco

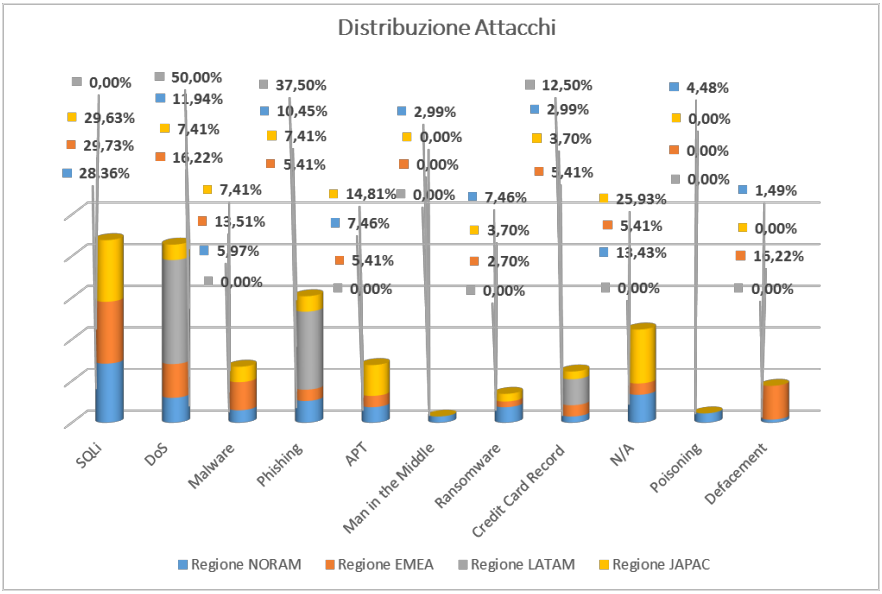

Figura 9: Tipologia di attacco per area

La distribuzione degli attacchi per regione mostra quanto l'America Latina sia sensibile agli attacchi DDoS e di Phishing, mentre sembra del tutto immune da attacchi del tipo SQL injection. È sempre bene tener presente che molto spesso le informazioni non vengono divulgate, infatti, la percentuale degli attacchi non definiti è essa stessa molto elevata.

Possono essere messe a punto delle attività illecite che, a differenza di quelle sopra elencate, utilizzano dei software, suite specifiche che vengono diffuse nel Dark Web, dove spesso

sono messi in vendita pacchetti di malware o exploit-zero-day capaci di rappresentare un danno per individui e aziende.

6. CYBER RISK E MERCATI FINANZIARI

Misurare l'effetto sul valore di un evento economico di un'impresa è, per molti, un'attività impegnativa. Tale misurazione è effettuata attraverso il ricorso a un'analisi di natura Event Study (Studio d'evento). Questa tecnica, basata su un metodo di analisi di tipo econometrico, è finalizzata alla valutazione dell'impatto esercitato da uno specifico evento sul valore di un'azienda attraverso l'uso di dati di natura finanziaria, ossia verificando le variazioni del corso delle azioni in seguito ad un evento inatteso. Se sono valide le ipotesi di efficienza dei mercati, ovvero che i prezzi riflettono istantaneamente le nuove informazioni disponibili, l'analisi della variazione dei prezzi dei titoli rappresenta un riflesso della variazione dei futuri cash flow attesi dell'azienda.
Quindi, osservando i prezzi dei titoli in un periodo circoscritto nel quale si rendono disponibili le informazioni in merito ad un determinato evento inatteso ed analizzando l'ampiezza della performance inattesa, si può inferire la significatività statistica su tale evento ed il suo impatto.
A differenza di altre tecniche di analisi, questa è effettuata ex-post, dopo l'annuncio di un evento. In questo modo, è possibile

comprendere al meglio, grazie a dati certi, quale sia stato l'effettivo impatto di un evento sul corso dei titoli. Nonostante essa sia effettuata successivamente al verificarsi di un dato evento, ha valore previsionale, in quanto, se si registrassero delle regolarità nei risultati, sarebbe possibile aspettarsi in futuro un impatto quantomeno simile.

Ad esempio, negli anni Novanta, si notò come le aziende, semplicemente modificando la propria denominazione, aggiungendo banalmente il suffisso ".com", registrassero delle anomalie nella performance dei propri titoli. Infatti, negli USA, una media di sette aziende al mese apportarono tale cambiamento nel 1999. Il prezzo azionario, quindici giorni prima della variazione di denominazione era di $2,79. Dopo tale evento, venne raggiunto il prezzo di $4,20 e un significativo incremento degli scambi. Questo fenomeno, noto come "La Bolla di Internet" fu registrato attraverso un'analisi Event Study eseguita da Cooper, Dimitrov e Rau nel 2001 che mostrarono come tale modifica facesse registrare ritorni anomali rispetto alla normale performance raggiunta prima del cambio di denominazione. Gli investitori, dunque, per un breve periodo poterono speculare su tale informazione, ma come spesso avviene nel mercato, fu possibile solo nel breve periodo, infatti la tecnica, non ebbe più successo dal 2001.

In sintesi, la metodologia consiste nella selezione di uno o più eventi di interesse nonché di un gruppo di titoli sui quali concentrare l'analisi. Per poter affermare che un dato evento abbia avuto un impatto significativo sui titoli in esame, è necessario confrontare i rendimenti dei titoli stessi nel momento in cui l'evento si è verificato, quindi i rendimenti effettivi, con i rendimenti attesi in assenza dell'evento, ovvero i rendimenti normali.

La scelta dell'evento da analizzare è molto importante, infatti, nonostante l'analisi sia molto flessibile in merito, è necessario isolarlo da altri avvenimenti di maggiore importanza che potrebbero aver determinato degli split azionari quello stesso giorno.

Il primo passo è quello di identificare la finestra temporale (event window), ovvero il periodo in cui saranno esaminati i prezzi dei titoli delle aziende soggette all'evento e la finestra di stima che serve a capire il comportamento del titolo in condizioni normali.

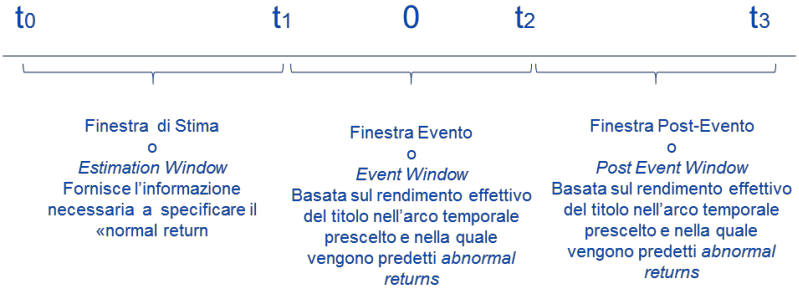

Figura 10:Finestre di analisi

In secondo luogo, è necessario un criterio di selezione per l'inclusione delle aziende nel campione. Per far sì che i risultati non presentino delle anomalie indotte, ovvero che i risultati siano influenzati da errori commessi dall'analista stesso, ad esempio inserendo aziende che hanno registrato delle perdite troppo inferiori rispetto alla media del campione e che quindi nei risultati sarebbero quelle con valore troppo basso per poter generare paragone, è necessario porre un criterio di scelta.

In seguito, prima di procedere con l'analisi e verificare attraverso dei test statistici la veridicità di quanto determinato, si stimano i rendimenti normali del titolo.

I rendimenti normali sono quei rendimenti che l'azione avrebbe registrato se l'evento non si fosse mai verificato. Per far ciò, nel corso degli anni, dal primo studio di questo genere effettuato da Eugène Fama del 1969, le tecniche statistico-economiche si sono evolute, dando vita a diversi modelli che, impiegando

svariati metodi di stima statistica, sono riusciti a coniugare la scienza finanziaria con i modelli previsionali, diventando sempre più precisi nell'individuare l'ipotetico andamento di un titolo in assenza di eventi di shock.

Il calcolo del rendimento normale viene effettuato all'interno della finestra di stima che viene isolata dal periodo dell'accadimento dell'evento in questione. Si immagini che il famoso lunedì nero del 19 ottobre 1987 non fosse mai avvenuto, in tal caso, il Dow Jones Industrial Average non sarebbe mai crollato di 508 punti e non avrebbe mai perso il 22% del suo valore totale, dunque il rendimento normale è il valore previsto in assenza di shock e la finestra di stima è il periodo immediatamente precedente all'evento, prima che questo inizi a produrre i suoi effetti.

In un'analisi Event Study, dopo aver calcolato il normal return, si procede con la registrazione degli effetti dell'evento, quindi il rendimento effettivamente realizzato nella event window (finestra evento), ovvero il periodo fissato dall'analista che racchiude il momento dell'annuncio o della diffusione della notizia che ipoteticamente possa variare i corsi azionari.

Questo campione è costituito da 60 aziende e istituzioni quotate colpite da eventi di tipo cyber. La selezione, cioè il criterio di scelta sulla base del quale sono assunte delle imprese da analizzare, è stata effettuata a seconda dei relativi annunci

e in base alla perdita generata dall'evento di almeno un milione di dollari.
Il database utilizzato è del sito web "Hackmageddon". I dati sono stati scorporati manualmente in base ai criteri sopra riportati.
L'output dell'analisi è dato dai CAR (Rendimenti Anomali Cumulati), che sono stati calcolati in relazione all'evento.

L'interpretazione è molto intuitiva. Quando questo valore è negativo, l'impatto di quel dato evento è negativo, ovvero ha modificato il corso azionario generando un ribasso del prezzo di un titolo. L'ampiezza del valore deve essere necessariamente rapportata alle oscillazioni dei prezzi precedenti, se un titolo, ha lievi oscillazioni di prezzo nel suo tracciato storico, è difficile che il livello del CAR sia molto elevato.

Per questa motivazione, sono presentate delle distribuzioni di questi valori all'avvicinarsi del giorno dell'evento, partendo dalla prima finestra (-10,+2), ovvero dieci giorni prima dell'evento, a 2 giorni dopo, fino a (-1,+1).
Di seguito:

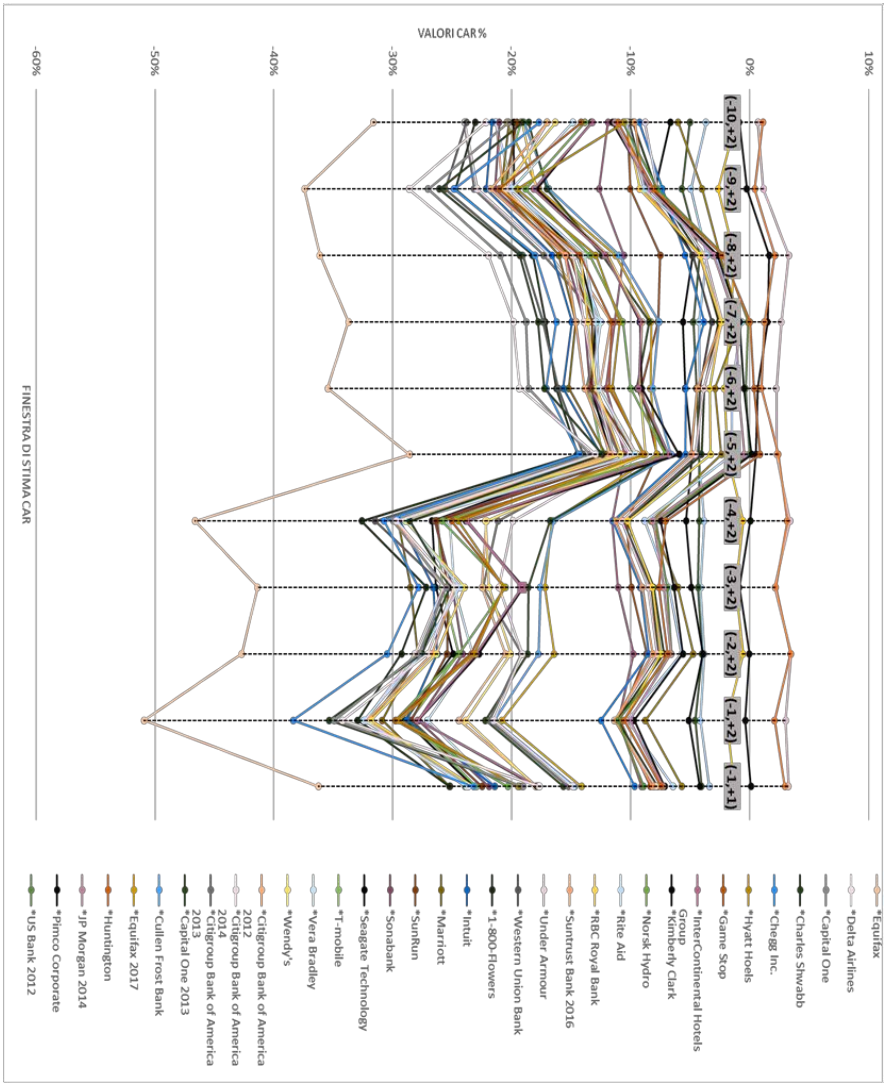

Figura 11: Valori CAR comparati attacco cyber

L’analisi come già indicato in precedenza è stata condotta su un campione di 60 aziende. Si è pensato di riportare la descrizione solamente di alcuni casi per area in questo studio per fornire al lettore indicazioni sulla tipologia di evento e l’impatto causato sul valore azionario.

6.1. NORAM

Caso 1	
Data pubblicazione evento	7 settembre 2017
Azienda	Equifax Inc.
Settore	Finanziario
Tipologia attacco	Cyber-Crime, APT attraverso lo sfruttamento di una vulnerabilità Apache Struts (CVE-2017-5638)
Descrizione evento	Violazione informatica che ha messo a rischio i dati di 143 milioni di cittadini americani rubando nomi, date di nascita, numeri di previdenza sociale, carte di credito di oltre 209 mila persone e contenziosi di 182 milioni di consumatori. L’attacco effettivo risale al luglio 2017.

Descrizione impatto su valore azionario	Perdita del **19%** sul valore azionario, l'impatto è stato tra i peggiori delle aziende analizzate.

Caso 2	
Data pubblicazione evento	Reso noto alla SEC il 19 settembre 2018 – Reso noto al pubblico il 26 settembre 2018
Azienda	Chegg Inc.
Settore	Informazione
Tipologia attacco	Cyber-Crime, APT
Descrizione evento	Violazione informatica che, sfruttando la vulnerabilità dei sistemi di protezione, ha provocato la perdita di 40 milioni di dati sensibili degli utenti. La perdita di dati è avvenuta il 29 aprile dello stesso anno da parte di ignoti autori.
Descrizione impatto su valore azionario	L'impatto sul rendimento azionario è stato del **12%** in meno rispetto ai valori normali.

Caso 3	
Data pubblicazione evento	28 luglio 2019

Azienda	Capital One Financial Corp
Settore	Finanziario
Tipologia attacco	Cyber-Crime – Exploit Vulnerability - Hack
Descrizione evento	Rubate le informazioni a circa 100 milioni di clienti statunitensi e canadesi. Il danno quantificato ammonta a circa 150 milioni di dollari. L'attacco sarebbe opera di Page Thompson, arrestata dall'FBI ex dipendente di una famosa azienda del settore informatico.
Descrizione impatto su valore azionario	È possibile notare come la notizia sia stata notevolmente anticipata dagli investitori, le oscillazioni dei rendimenti sono molto contenute e all'avvicinarsi dell'evento, la variazione non si accentua, anzi i rendimenti restano negativi intorno al **-3%**

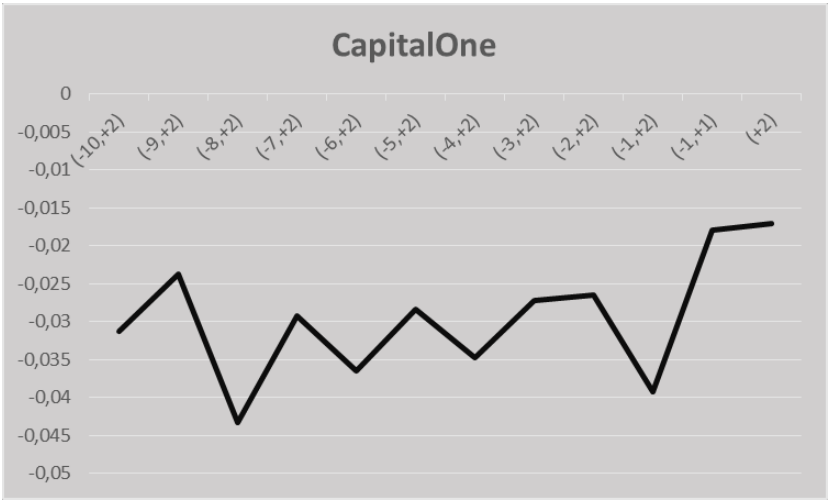

Figura 12: Caso CapitalOne

6.2. JAPAC

Caso 1	
Data pubblicazione evento	28 giugno 2019
Azienda	Mitsubishi Electric
Settore	Industriale - Elettronico
Tipologia attacco	Cyber Espionage – Vulnerabilità Zero Day
Descrizione evento	Sottratti dati interni dell'azienda, tra cui le informazioni di tutto il personale dipendente e 200 mb di informazioni di tipo aziendale-privato. L'attacco risalirebbe

	a mesi prima e si ipotizza sia stato effettuato da parte di alcuni hacker cinesi e coinvolgerebbe alcune personalità istituzionali. Le notizie in merito sono state limitate, ma sono state coinvolte ben 14 filiali della stessa azienda.
Descrizione impatto su valore azionario	In questo caso l'impatto azionario è stato molto contenuto. Facente parte tra le aziende che hanno riscontrato CAR positivi, è facile notare come la mancata divulgazione generi calma sui mercati.

Caso 2	
Data pubblicazione evento	29 marzo 2019
Azienda	Toyota Motor Corp.
Settore	Automobilistico
Tipologia attacco	Cyber Espionage, APT
Descrizione evento	L'attacco ha messo a rischio i dati di 3.2 milioni di utenti. È il più grave di una serie di attacchi effettuati da un gruppo di Hacker Vietnamiti, ovvero APT32,

	conosciuti anche come OceanLotus o Cobalt Kitty di cui restano ancora sconosciute le identità.
Descrizione impatto su valore azionario	L'impatto sul valore azionario rispetta la media del campione, come molti altri, la notizia è stata anticipata nei 5 giorni precedenti all'evento, infatti, questo attacco, essendo parte di una serie di operazioni di un gruppo Hacker, lascia che il rendimento AR(anormale) si attesti al **-2%** senza particolari oscillazioni.

Caso 3	
Data pubblicazione evento	19 Giugno 2011
Azienda	SEGA
Settore	Videogames - Elettronica
Tipologia attacco	Cyber Crime - Unauthorized access
Descrizione evento	Rubati i dati di circa 1.5 milioni di utenti. La comunicazione da parte dell'azienda è stata contestuale alla perdita. L'attacco è stato effettuato da hacker ignoti. Lulz Sec, coinvolto in diversi attacchi informatici

	verso piattaforme analoghe come Nintendo, ha negato il coinvolgimento.
Descrizione impatto su valore azionario	La notizia, come nel caso Toyota è anticipata, questo non permette di effettuare extra rendimenti maggiori del 2%

6.3. EMEA

Caso 1	
Data pubblicazione evento	28 gennaio 2016
Azienda	HSBC
Settore	Bancario
Tipologia attacco	Cyber Crime - DDos
Descrizione evento	Interruzione dei sistemi e perdita di dati sensibili. L'annuncio è stato contestuale all'evento a causa dell'impossibilità dell'utilizzo dei servizi di internet banking. Nonostante le rassicurazioni da parte del colosso, gli effetti sono stati notevoli.
Descrizione impatto su valore azionario	

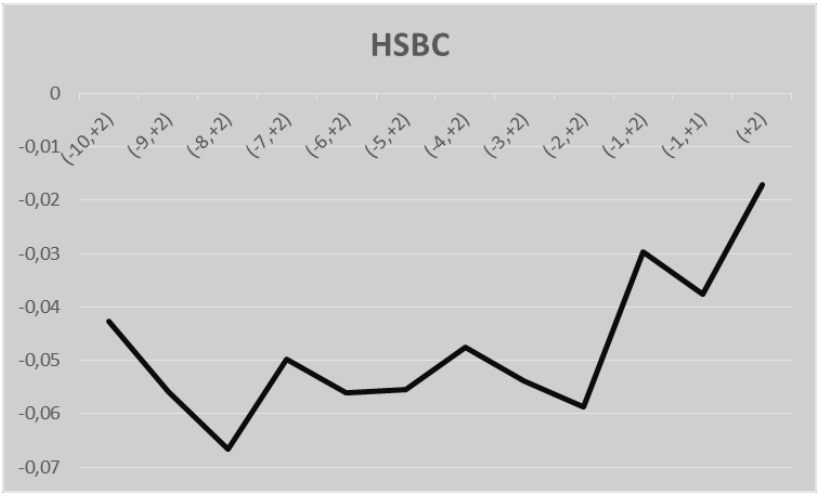

Figura 13: Caso HSBC

Caso 2	
Data pubblicazione evento	28 giugno 2018 presunto attacco – 2 luglio 2018 Data Ufficiale
Azienda	Adidas
Settore	Abbigliamento - Sportivo
Tipologia attacco	Unauthorized Access
Descrizione evento	Annuncio di ipotetica violazione confermata con un comunicato stampa ufficiale del 2 luglio dello stesso anno. Il

	coinvolgimento di milioni di clienti era noto fin dal momento dell'avvertimento del presunto attacco.
Descrizione impatto su valore azionario	L'impatto sui rendimenti si è verificato il giorno dell'annuncio del presunto attacco e non il giorno del comunicato stampa ufficiale, infatti, allo stringersi della finestra evento i rendimenti non subiscono fluttuazioni al ribasso. Si perde un rendimento di circa il **4%** il 28 giugno.

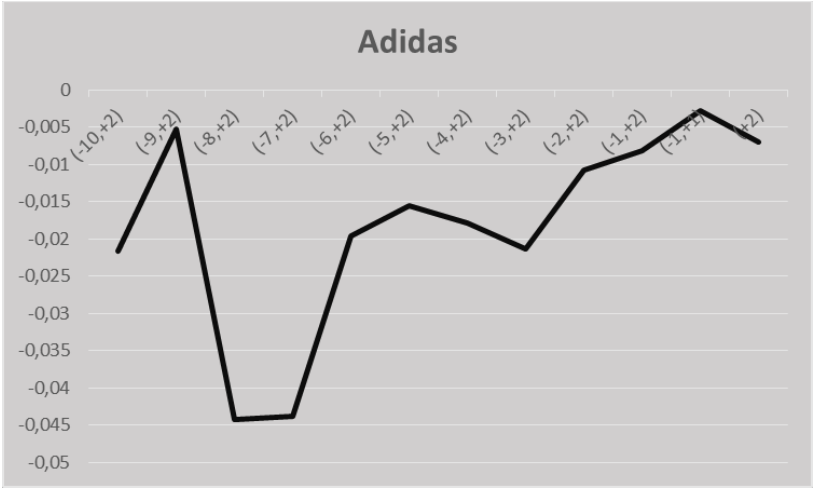

Figura 14: Caso Adidas

Caso 3	
Data pubblicazione evento	19 marzo 2019
Azienda	Norsk Hydro
Settore	Industria - Metallurgica
Tipologia attacco	Cyber Crime - Ransomware
Descrizione evento	L'attacco ha generato un blocco nella produzione di alluminio e dell'uso degli impianti di laminazione dell'azienda lo stesso giorno dell'annuncio, influenzando l'intero settore industriale.
Descrizione impatto su valore azionario	Le conseguenze sono state devastanti intra-day. La variazione si è estesa all'intero settore metallurgico, modificando le quotazioni verso l'alto dell'alluminio sulla London Metal Exchange. A differenza delle altre aziende prese in esame, la variazione è stata giornaliera. Si può notare come il rendimento percentuale diminuisca sempre di più allo stringersi della finestra evento, andando ad attestare una perdita

	tra il **7** e il **9%**. Nei due giorni subito successivi invece, il valore tende ad andare verso l'alto, quasi a normalizzarsi, nuovamente segnando una non permanenza nella perdita legata a questo evento. Esso persisterebbe e continuerebbe ad essere al ribasso se le conseguenze dell'attacco fossero permanenti e di lungo periodo e se gli investitori ne fossero a conoscenza, in questo caso è palese come al passare dell'evento, immediatamente il rendimento torni verso l'alto.

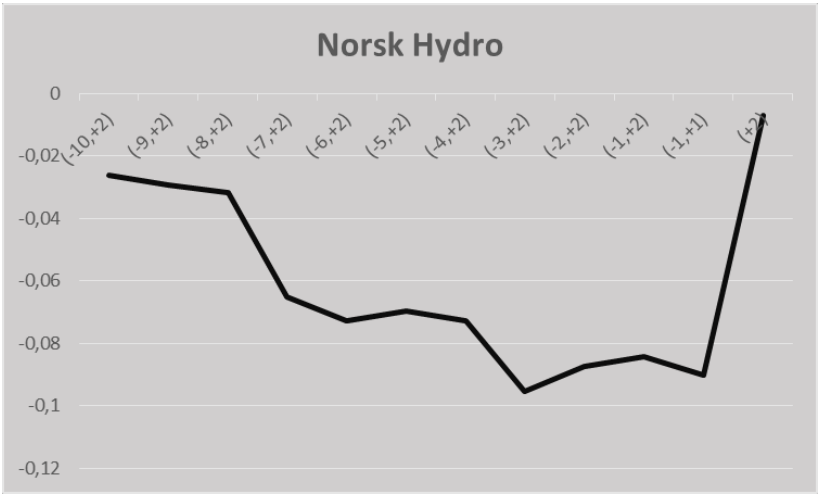

Figura 15: Caso Norsk Hydro

6.4. LATAM

Per la regione Latam non è stato possibile produrre dei risultati per quanto concerne l'impatto azionario. Infatti, la regione si presenta bersaglio di attacchi informatici di tipo istituzionale, dunque sono maggiormente prese di mira personalità politiche o organi di difesa nazionali, infatti, tra le regioni analizzate, su 220 attacchi presi in considerazione totali, il tasso di cyber espionage della regione LATAM è il più elevato e i paesi più colpiti risultano essere Brasile e Argentina.

7. RISULTATI

La verifica dell'impatto di un evento sui corsi azionari è una attività in continua evoluzione, questa cerca di fondere il comportamento atteso degli investitori a tecniche di analisi di tipo statistico-economiche.
Si può notare come vi sia un'interruzione ben definita per molti corsi azionari circa 5 giorni prima dell'annuncio ufficiale, dunque la circoscrizione della finestra è stata efficace a carpire l'impatto.
L'impatto c'è, ed è negativo. La sua rilevanza dipende da quanto l'oscillazione sia stata elevata rispetto alle oscillazioni normali. Questa variazione, non è permanente, anzi viene velocemente assorbita all'avvicinarsi dell'evento. Come mostrato dagli esempi fatti in precedenza, il valore azionario muta a seconda del caso specifico. Generalmente è possibile dire che in assenza di altri fattori determinanti, il rendimento diminuisce almeno del 7% in presenza di un attacco informatico, ovviamente dipende anche dalla sua portata e da come e se la notizia venga divulgata.
Spesso, gli annunci ufficiali vengono ritardati in vista di un contenimento delle perdite, ma, la dispersione delle informazioni è un elemento che non può essere controllato dalle imprese.

Molti annunci presenti nel campione analizzato, come ad esempio il primo del 2017 di Equifax è stato reso ufficiale solo a settembre dello stesso anno, in riferimento ad un attacco subito nel 2015 e poi nel luglio dello stesso anno. L'obiettivo di legare questi eventi al rischio è legato al fatto che le aziende adoperano queste scelte di annuncio ritardato spesso per non incorrere in altri tipi di rischi come, ad esempio, il rischio reputazionale che incrementa quando le istituzioni o le aziende perdono di credibilità.

Un esempio è stato lo scandalo Facebook-Analytica, un utilizzo di dati senza autorizzazione, iniziato nel 2015 e divenuto ufficiale solo nel marzo 2018, generando un fortissimo crollo non solo azionario, ma anche reputazionale elevatissimo.

In questa sede si sono approfonditi i rischi derivanti da attacchi esterni nei confronti di aziende quotate.

Per speculare in presenza di un attacco informatico da semplice investitore è più complesso di quanto non lo sarebbe per un'impresa. Il possesso di un'informazione privilegiata permetterebbe di muoversi in anticipo rispetto al mercato, ad esempio ritardare la pubblicazione di un annuncio e vendere al contempo la maggior parte delle proprie azioni è una tecnica molto diffusa per evitare grosse perdite. Altre volte, la divulgazione delle notizie pochi secondi prima, attraverso un algoritmo può portare enormi guadagni, si pensi allo scandalo della Bank of England del dicembre 2019 dove gli hacker

fornivano accesso a file audio privati contenenti notizie sui tassi di interesse.

La fluttuazione dei prezzi dipende sempre da eventi che colpiscono l'azienda in esame, ciò avverrebbe anche nei confronti degli stati, i cui titoli seguono logiche intrinseche ad eventi politici ed economici. Sono noti diversi attacchi informatici che hanno mirato a personalità politiche al fine di rovinarne la reputazione personale, del partito politico di appartenenza o dello stato che si trovavano a rappresentare. La difficoltà in questi casi sta nell'isolare l'evento tra i molteplici che interessano gli stati e colpiscono questi ambiti, cosa che è invece possibile attraverso i prezzi intra-day delle corporate. La difficoltà di questa analisi sta nel limitato ambito di applicazione e dalla necessità di reperire una data certa per la costruzione delle stime. La stessa difficoltà relativa alle tempistiche che dovrebbero avere coloro che intendono battere il mercato attraverso l'utilizzo di informazioni di tipo riservato. Gli attacchi informatici sono difficili da prevedere e contemporaneamente difficili da quantificare. A questo punto intervengono le misure di policy che tendono a penalizzare chi ha dei sistemi deboli di quantificazione preventiva interna.

L'impatto è senza dubbio palese sui corsi azionari, purtroppo però, il fair game del mercato azionario è quasi una costante e per battere il mercato sono necessari e imprescindibili tempo e conoscenza e perché no, anche un po' di fortuna.

8. BIBLIOGRAFIA

- Ponemon Institute (2016), Cost of Data Breach Study: Global Analysis, Ponemon Institute Research Report, June 2016.
- Ponemon Institute (2018), Cost of Data Breach Study: Impact of Business Continuity Management, Ponemon Institute Research Report.
- Ciciretti, R., Iori M., Trenta U. (2018), "Eventi e News nei Mercati Finanziari", Seconda Edizione, Giappichelli Editore
- Office of Financial Research (2016), "Cybersecurity and Financial Stability: Risks and Resilience", View Point.
- Office of Financial Research (2017), "Cybersecurity and Financial Stability: Risks and Resilience", OFR Viewpoint
- Peterson, (1989), "Event studies: A review of issues of methodology" Journal of Business and Economics (Peterson).
- Clusit, "Rapporto sulla sicurezza informatica 2019".
- Seiler, M. J. (2000), "The Efficacy of Event Study Methodology Measuring Ereit Abnormal Performance Under Conditions of Induced Variance", Journal of Financial and Strategic Decisions, Vol. 13, n. 1.
- Certified Ethical Hacker, (2017) "Advanced Hacker Course", CEH Council.

- Hackmageddon (2019), Database Attacchi Informatici 2011, .com/2011-cyber-attacks-timeline-master-index/
- Hackmageddon (2019), Database Attacchi Informatici 2012., .com/2012-cyber-attacks-timeline-master-index/
- Hackmageddon (2019), Database Attacchi Informatici 2013 .com/2013-cyber-attacks-timeline-master-index/
- Hackmageddon (2019), Database Attacchi Informatici 2014 .com/2014-cyber-attacks-timeline-master-index/
- Hackmageddon (2019), Database Attacchi Informatici 2015. .com/2015-cyber-attacks-timeline-master-index/
- Hackmageddon (2019), Database Attacchi Informatici 2016. .com/2016-cyber-attacks-timeline-master-index/
- Hackmageddon (2019), Database Attacchi Informatici 2018. .com/2018-cyber-attacks-timeline-master-index/
- Hackmageddon (2019), Database Attacchi Informatici 2019. .com/2019-cyber-attacks-timeline-master-index/
- IlSole24Ore (2019), Sicurezza Informatica, https://www.ilsole24ore.com/art/sicurezza-informatica-ecco-titoli-che-guadagnano-borsa-i-cyber-attacchi-AEEX3jMB?refresh_ce=1

AUTORI

MARIKA MAZZA

Marika Mazza, laureata magistrale in Analisi Economica presso l'Università degli Studi di Roma "La Sapienza" e analista finanziaria presso una importante banca depositaria su scala globale. Amplia e approfondisce l'ambito dell'analisi econometrica e le sue applicazioni nella macro-area finanziaria. Collabora con GCSEC per verificare gli effetti sui mercati finanziari degli eventi di violazione della sicurezza informatica.

MASSIMO CAPPELLI

Massimo Cappelli è responsabile della funzione cyber intelligence all'interno del Computer Emergency Response Team del Gruppo Poste Italiane nonché Operations Planning Manager della Fondazione Global Cyber Security Center. In passato ha lavorato come consulente presso Booz Allen Hamilton e Booz & Company nella practice Risk Resilience and Assurance.