Dipartimento di Impresa e Management

Cattedra: Organizzazione dei sistemi informativi aziendali

Studio ed analisi dell'information security nelle organizzazioni: casi a confronto

RELATORE
Prof. Paolo Spagnoletti

CANDIDATO
Giuseppe Catone
177161

ANNO ACCADEMICO 2014/2015

Sommario

Abstract **5**
1. La sicurezza nelle organizzazioni. Aspetti generali. **7**
2. Background teorico **13**
2.1 Incident risk analysis. **13**
2.2 TFI model. **16**
2.3 Bilanciamento strategico tra prevenzione e risposta. **19**
3. Analisi dei casi. **26**
3.1 Metodi e finalità di ricerca **26**
3.2 Caso uno: TJX Companies, Inc. **27**
3.3 Caso due: Target Corporation. **29**
3.4 Caso tre: Home Depot, Inc. **33**
3.5 Caso quattro: J.P. Morgan Chase & Co **36**
3.6 Caso cinque: Heartland Payment Systems Inc. **40**
3.7 Caso sei: eBay Inc. **43**
3.8 Caso sette: Adobe Systems Inc. **46**
3.9 Caso otto: SK Communications **48**
3.10 Caso nove: Evernote Corporation. **51**
3.11 Comparazione dei casi. **54**
4. Conclusioni finali. **60**
5. Appendice **62**
Bibliografia **93**
Sitografia **94**

Abstract

In un contesto organizzativo dove la tecnologia la fa da padrona, il tema della sicurezza informatica sta prendendo sempre più piede. Un numero sempre maggiore di organizzazioni si affida alle nuove tecnologie e sempre una maggior parte di queste sente la necessità di dover rendere sicuro un ambiente di tale importanza sia strategica che operativa. Non a caso difatti la maggior parte di queste organizzazioni spende un'ingente somma di denaro sotto la voce "sicurezza informatica". Nonostante ciò però, negli ultimi anni si è osservato un forte aumento del numero di incidenti, i quali hanno causato la perdita di un elevato numero di informazioni di rilevante importanza strategica. Vista quindi l'importanza di tale tematica, negli ultimi tempi sono state elaborate diverse teorie, le quali hanno cercato di fornire una visione più chiara, ordinata e schematica di tali eventi al fine di poter disporre di metodologie per la gestione e il contenimento del rischio informatico. In questo contesto, si è quindi deciso di combinare alcune di queste teorie con lo scopo di ottenere un quadro di riferimento teorico preciso ed affidabile con la quale effettuare delle analisi empiriche relative ad alcuni dei più grandi incidenti della storia. Questi casi saranno analizzati secondo diverse prospettive, in modo tale da fornire al lettore una visuale a 360 gradi del loro contesto operativo, per poi evidenziare quegli elementi comuni e discordanti che caratterizzano il proprio approccio alla gestione del rischio. Come risultato di tale lavoro, si avrà che, ogni organizzazione adotterà un proprio specifico approccio alla gestione del rischio, il quale sarà però caratterizzato da fattori specifici come: il contesto operativo, il livello di tecnologia adottato e la quantità e qualità di dati da questi posseduti. Le organizzazioni saranno così suddivise in tre macro classi; quelle affrontano tali rischi tramite un approccio maggiormente volto alla prevenzione, quelle che preferiscono concentrare i propri sforzi su una risposta efficiente, dandogli quindi un maggior peso rispetto alla prevenzione, o quelle che necessitano di adottare un bilanciamento strategico tra i due paradigmi.

1. La sicurezza nelle organizzazioni. Aspetti generali.

In un mondo in costante crescita, in costante evoluzione come il nostro, può ritenersi impensabile che un'organizzazione, specie se di grandi dimensioni, non si avvalga dell'ausilio della tecnologia nello svolgimento delle proprie operazioni quotidiane. In un mondo sempre più interconnesso e tecnologicamente avanzato, ogni piccola operazione necessita di un supporto informatico o quantomeno di essere informatizzata. In un mondo dove però il supporto tecnologico è alla base della maggior parte delle interazioni quotidiane, i rischi per la sicurezza si amplificano a dismisura. Trascurando gli aspetti più generali della sicurezza informatica e concentrandoci sul concetto di sicurezza nelle organizzazioni, questa va intesa come la protezione dell'intera struttura tecnologica e delle informazioni archiviate al suo interno.

Per protezione deve intendersi tanto la protezione fisica quanto quella digitale e, tanto più è grande un'organizzazione, tanti più dati questa gestisce, tanti più rischi questa corre. Tali rischi comprendono non soltanto quelli che, erroneamente, nell'accezione comune vengono definiti come "rischi informatici", ad esempio accessi non autorizzati o una negazione del servizio. Ci si riferisce invece, anche a quei rischi più propriamente fisici, come ad esempio, il rischio di incendio o di allagamento delle strumentazioni informatiche. Ancora, si potrebbe incorrere nel rischio che un computer non risponda ai comandi o, peggio ancora, che un dipendente possa appropriarsi, direttamente o indirettamente, di informazioni, dati o strumentazioni proprie della società. In particolar modo quando si parla di organizzazioni che, per il proprio business, raccolgono grandi quantità di dati, la sicurezza dell'*Information Technology* (IT) deve sempre essere posta in primo piano. La rilevanza che tale tematica ha assunto negli ultimi anni, dato anche l'elevato numero di incidenti verificatosi proprio in questo settore, il quale ha causato gravi perdite sia in termini di sicurezza delle informazioni che in termini monetari, è stata tale da spingere numerose organizzazioni sia pubbliche che private (in particolar modo negli Stati uniti) ad istituire standard ed enti che operano con il fine di garantire una maggiore sicurezza delle strutture informatiche.

Un primo rilevante squillo di tromba in questa direzione, è arrivato nel lontano 1947, con la creazione degli standard ISO (International Organization for Standardization), i quali si

propongono di promuove standard proprietari, industriali e commerciali in tutto il mondo[1]. Altro segnale della necessità di una standardizzazione del settore può scorgersi con la creazione del Control Objectives for Information and related Technology (COBIT) il quale è un modello (framework) per la gestione della *Information and Communication Technology* (ICT), creato nel 1992 dall'associazione americana degli auditor dei sistemi informativi (Information Systems Audit and Control Association - ISACA), e dal IT Governance Institute (ITGI)[2]. Nella sicurezza del settore commerciale e, in particolar modo nella sicurezza dei pagamenti elettronici, una svolta epocale la segnano gli standard PCI DSS. Istituiti nel 2004, si propongono come standard di sicurezza aggiuntivo, con il fine di garantire la protezione dei dati in transito nel momento in cui si verifichi un pagamento tramite carta di credito[3]. Chiaramente queste sono solamente alcune delle numerose organizzazioni e di standard esistenti sia nel settore privato che in quello pubblico, i quali si occupano di garantire standard di sicurezza sempre aggiornati e accessibili.

Relativamente ai rischi tecnologici che questi si propongono di eliminare, bisogna ricordare che, come detto poc'anzi, i rischi di un'organizzazione non sono "limitati" a possibili attacchi informatici, bensì bisogna tenere in considerazione numerose altre variabili, interne all'organizzazione che potrebbero dar luogo alla perdita di informazioni. A tal proposito, viene in soccorso una ricerca condotta da Risk Based Security, Inc [13], la quale mette in evidenza come una grande porzione di incidenti abbia origine proprio dall'interno dell'impresa.

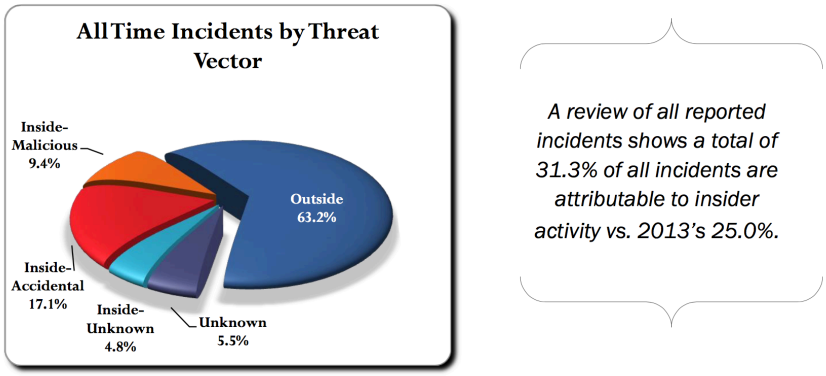

Figura 1.1 Origine degli attacchi in percentuale. [13]

[1] International Organization for Standardization. http://en.wikipedia.org/wiki/International_Organization_for_Standardization

[2] COBIT. http://it.wikipedia.org/wiki/COBIT

[3] Payment Card Industry Data Security Standard. http://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard

Si sente quindi il bisogno di adottare misure preventive a tali eventi, dannosi per l'intera organizzazione. Tralasciando per il momento il rischio relativo ad attacchi informatici provenienti dall'esterno dell'organizzazione e, concentrandoci su quelli che possono avere origine interne, possiamo distinguere in:

- Rischio di attacchi interni malevoli
- Rischio di attacchi interni accidentali
- Altri rischi di derivazione non umana

I primi, sono solitamente messi in atto dal personale, il quale tenta di appropriarsi di informazioni proprie dell'impresa con lo scopo di ottenerne un ricavo personale. Chiaramente questo tipo di rischio non è necessariamente connesso con la sicurezza dell'IT o con i dati posseduti dall'azienda ma può essere esteso ad ogni tipo di attività. Risulta lampante l'esempio del cassiere che potrebbe fuggire con l'incasso giornaliero.

Per quanto riguarda gli attacchi interni accidentali, chiaramente questi non sono intenzionali da parte di chi li pone in essere ma, nonostante ciò potrebbero causare rilevanti danni per l'intera organizzazione. Anche questo tipo di attacchi non è necessariamente riferibile alla sicurezza IT, in quanto potrebbe ad esempio verificarsi che per negligenza un dipendente possa dimenticarsi di chiudere a chiave la cassetta di sicurezza. Ancora, potrebbe accadere che, un dipendente possa accidentalmente aprire un'email contenente un malware il quale sia capace di bloccare l'intero sistema ed entrare in possesso delle informazioni da questo possedute.

Infine, potrebbe accadere anche che, a causa di eventi naturali (come un allagamento o un incendio) e quindi senza che vi sussista un errore umano, possano essere compromesse le strumentazioni informatiche, come i server o le postazioni del personale. In questo ultimo caso risulta utile redigere un piano di sicurezza, proprio per evitare la perdita di informazioni derivante da tali eventi. Uno di questi potrebbe essere il *Disaster Recovery Plan,* il quale viene inserito nel più ampio documento del *Business Continuity Plan* redatto appunto con lo scopo di garantire un più veloce e sicuro recupero delle informazioni perse durante l'incidente.

Nonostante la grande attenzione posta sul tema e la forte cooperazione fra numerose aziende però, gli incidenti nell' IT non sembrano cessare anzi, sembrerebbero essere in costante aumento. Come esposto dalla su citata ricerca, il numero di incidenti ha subito una notevole accelerazione nel corso degli ultimi anni, probabilmente a causa della sempre maggiore

accessibilità alle risorse tecnologiche sia da parte delle imprese che dei consumatori ma, più probabilmente a causa della sempre maggiore rilevanza e del sempre maggior numero di dati posseduti da organizzazioni pubbliche e aziende private. Possiamo affermare infatti che, tanti più dati possiede un'organizzazione (pubblica o privata che sia), tanto più questa sarà soggetta ad attacchi informatici (i quali chiaramente costituiscono il pericolo maggiore). Questo perché tramite un attacco di questo genere, si ha la possibilità di entrare in possesso di un elevato numero di informazioni, le quali potrebbero essere sfruttate direttamente (ad esempio tramite accessi non autorizzati su i conti bancari dei consumatori) o indirettamente (ad esempio tramite la vendita di questi sul mercato nero). L'istogramma sottostante, illustra chiaramente il numero di dati sottratti in ogni periodo indicato. Prendendo come esempio l'anno 2013, risulta chiaro come, nonostante il numero di incidenti sia sceso di quasi 1/3 rispetto all'anno precedente, il numero di dati sottratti si è più che triplicato nello stesso periodo. Questo mette in risalto che, un piccolo numero di organizzazioni sia in possesso di un elevato numero di dati; pertanto più le organizzazioni sono di grandi dimensioni (e quindi in possesso di un più elevato numero di tati), più queste risultano in pericolo. Come esempio chiarificatore possiamo considerare il caso Adobe, famosa società operante nell'ingegneria del software, che, a seguito di un attacco, ha esposto 150 milioni di dati riferibili ad altrettanti clienti.

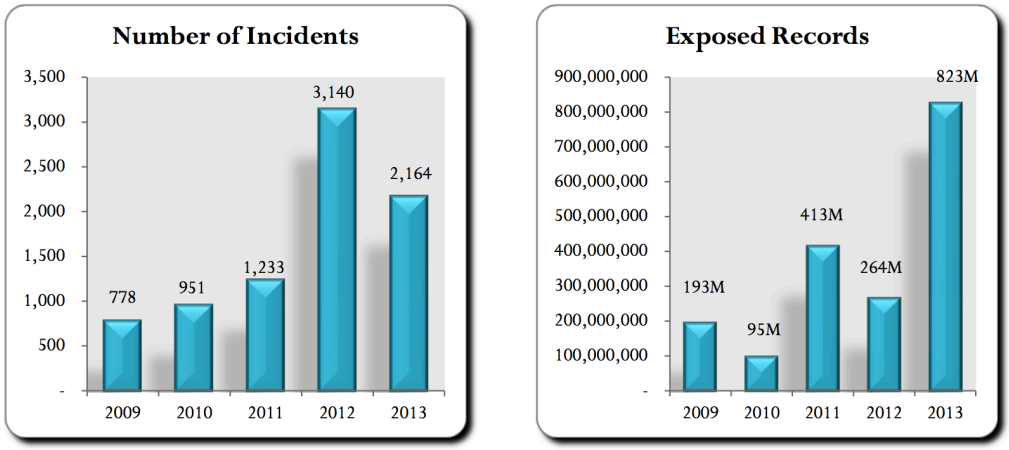

Figura 1.2 Numeri di dati persi tra il 2009 e il 2013. [13]

Oltre che dal punto di vista della destabilizzazione dell'intera organizzazione e della violazione della privacy che può conseguire ad eventi di questo genere, bisogna tenere a mente anche l'enorme costo che questi eventi possono generare.

Ogni anno, le più grandi organizzazioni stanziano ingenti somme di denaro al fine di garantire la sicurezza dell'IT ma, chiaramente, a prescindere dalla rilevanza di questi stanziamenti, i rischi vengono corsi continuamente e, questo si amplifica oltre che per causa della grandezza dell'organizzazione, anche in proporzione al tipo di tecnologia adottata e alla posizione di mercato occupata.

Un incidente informatico, può quindi avere forti ripercussioni anche in termini economici sull'intera organizzazione. Nel calcolo del costo complessivo a seguito di un incidente, vanno considerati sia i costi diretti (ovvero quelli direttamente connessi all'incidente, come il costo del personale addetto al ripristino dello status quo, il costo derivante da eventuali azioni legali, il costo delle indagini ecc.) che quelli indiretti (come il deprezzamento del titolo nel caso si trattasse di una società quotata o un abbassamento del livello di reputazione posseduto dall'organizzazione).

Una ricerca condotta da Ponemon Institute [15], su alcuni data breach verificatesi nel 2011 stabilisce che: "*For the first time in seven years, both the organizational cost of data breach and the cost per lost or stolen record have declined. The organizational cost has declined from $7.2 million to $5.5 million and the cost per record has declined from $214 to $194"*. Tralasciando quindi il fatto che, nell'anno 2011 si sia verificato una diminuzione sia del costo totale che del costo pro capite per record persi (da precisare che in questo caso, con "record" si intende "as information that identifies an individual whose information has been compromised in a data breach" [15]), risulta interessante osservare che i costi di ciascun data breach appaiono decisamente ingenti. Bisogna inoltre tenere presente che, dato l'anno di pubblicazione della ricerca e dato il periodo di riferimento di questi incidenti, è stato possibile osservare solo gli effetti di breve periodo, trascurando così quelli di medio e lungo termine, i quali in alcuni settori (primo fra tutti quello tecnologico) potrebbe causare pesanti ripercussioni sulla stabilità societaria (specie per quelle aziende di piccole-medio dimensioni o neonate, le quali devono ancora affermarsi sul mercato di loro competenza). Bisogna inoltre tenere presente che nella ricerca sono stati analizzati solamente data breach che hanno coinvolto un numero di record inferiore alle 100.000 unità e che quindi tali risultati non considerano i costi sostenuti da quelle società che hanno dovuto affrontare dei "catastrophic breaches". Attraverso la figura 1.3 inoltre, è possibile osservare come sia suddiviso il costo pro capite di ogni data breach per settore in cui le aziende colpite operano.

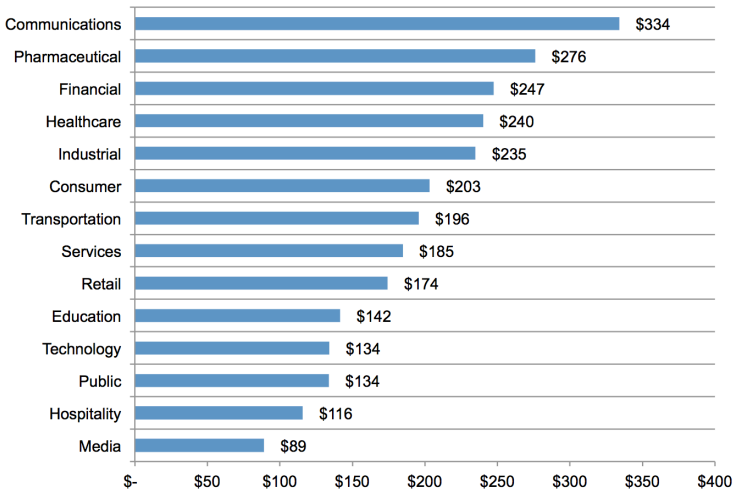

Figura 1.3 Costo pro capite per classificazione di settore. [15]

Effettuato questo primo excursus sul tema e, presentata la tematica e la rilevanza della sicurezza dell'*Information Technology* nelle organizzazioni, risulta chiaro che la strada da percorrere per garantire un sufficiente livello di sicurezza delle informazioni sia ancora assai lunga. Si nota inoltre, la necessità della costituzione di enti di natura giuridica, dotati di poteri maggiormente pervasivi e di capacità ispettive e di controllo sul livello di sicurezza adottato nelle organizzazioni al pari di quegli enti attualmente esistenti e operanti nei paesi più sviluppati del mondo. Questo, al fine di garantire un maggior grado di sicurezza verso tutte quelle informazioni sensibili, riferibili a milioni di individui che, al giorno d'oggi data l'inarrestabile espansione della tecnologia e dei social network risultano ormai di pubblico dominio.

Questa tesi, si incentrerà sull'analisi empirica di alcuni dei più grandi ed emblematici incidenti informatici verificatesi nel corso degli ultimi anni. Questi sono ognuno caratterizzato da proprie specificità, derivanti dalla struttura organizzativa adottata, dal livello della tecnologia in azienda, dagli stanziamenti riservati alla sicurezza IT, dalla posizione di mercato occupata, dal core business della società e in particolar modo dal tipo di attacco subito. Tali eventi saranno osservati attraverso varie prospettive, proprio con l'intento di ottenere una più chiara visione della dinamica dell'accaduto, di ciò che è stato fatto o che si sarebbe potuto fare per rimediarvi e di ciò che è stato perso, seguendo lo schema ricorrente del modello Technical, Formal ed Informal (*TFI model*) [2] e quello del bilanciamento strategico tra prevenzione e risposta [1] che saranno presentati nel capitolo successivo. Tale esposizione, mira quindi a fornire un sostegno empirico, tramite un'analisi quantitativa, a tali teorie.

2. Background teorico

In questo capitolo verranno presentate alcune teorie proprie del risk management al fine di poter disporre dei riferimenti su cui si basa la struttura delle analisi empiriche effettuate.

2.1 Incident risk analysis. [3]

Preliminarmente presenteremo la Actor - Network Theory (ANT), la quale cerca di far luce sulle complesse e profonde interazioni di tutti quegli elementi caratterizzanti un'organizzazione, quali ad esempio: elementi sociali, umani, tecnologici, organizzativi, materiali e così via. Concetti centrali di questa teoria sono: la chiusura, la stabilizzazione, l'assunzione e l'allineamento. Con chiusura si intende quello status che si genera quando in un sistema chiuso (come potrebbe esserlo un'azienda) vi è consenso attorno ad una specifica tecnologia. La stabilizzazione invece è la resistenza al cambiamento che si genera quando la chiusura attorno ad una particolare tecnologia adottata, si stabilizza nell'organizzazione. Questa si realizza attraverso un processo di negoziazione e di assunzione - all'interno del sistema società - degli elementi e degli attori, caratterizzati da differenti caratteristiche proprie, per poi allinearli tra di loro inserendoli in un medesimo contesto e riuscendo così a combinare le caratteristiche proprie di ognuno di essi, al fine di ottenere l'output desiderato. Sin dalla sua nascita, la ANT e la sua ricerca, hanno visto applicazioni nella teoria manageriale, con la quale ci si focalizza su un singolo network attore e lo si allinea ed integra ad uno centrale e dominante. Le complessità emergono quando attori indipendenti tra di loro, tentano di allineare e far cooperare, network tra di loro differenti.

Bisogna tener conto che la complessità è una caratteristica costante della tecnologia e che secondo alcuni autori è proprio questa che la fa apparire autonoma da tutto il resto.

Di seguito presenteremo due teorie sull'argomento.

La prima è la Normal Accidents Theoy (NAT), la quale fu originariamente ideata da Charles Perrow (1984) [16]. Questa si basa su degli studi di sistemi tecnologicamente complessi dove anche un minimo errore potrebbe causare danni gravissimi. Il focus della teoria è incentrato

su disastri realmente accaduti, causati da sistemi tecnologicamente complessi come ad esempio l'incidente di Three Mile Island[4]. Al centro della NAT vi è la così detta "complessità interattiva", propria di sistemi tra di loro comunicanti e complessi. Perrow inizialmente pone però una distinzione tra le interazioni lineari e quelle complesse. Le prime, sono interazioni che si svolgono secondo una sequenza lineare, dove l'input di uno è dato dall'output del suo precedente. Dall'altra parte vi sono invece le interazioni complesse, le quali vengono ad esistenza quando sussistono percorsi ramificati, loop di feedback, "salti" su una sequenza lineare e così via. I componenti di queste interazioni si dicono strettamente collegati quando non esistono distanze tra l'operato dell'uno e del suo precedente, quindi il cambiamento di uno provoca l'immediato cambiamento del suo successivo. Ogni componente di un sistema potrebbe però comportarsi in modo inaspettato. Tale comportamento imprevisto, potrebbe interferire con un altrettanto comportamento inaspettato di altri componenti e così via, dando vita ad un effetto domino. Perrow afferma inoltre, che sistemi dotati di un alto grado di complessità, hanno maggiori probabilità di produrre interazioni impreviste, le quali potrebbero essere in grado di causare gravi danni al sistema nel suo complesso. Il grado di pericolosità di un danno, è dato dal numero di connessioni tra le varie componenti presenti nel sistema, infatti sistemi dotati di numerose connessioni interdipendenti tra di loro, hanno maggiori probabilità di produrre gravi errori rispetto a sistemi caratterizzati da minori connessioni. Pertanto, la NAT afferma che più è complesso un sistema, più vi sono connessioni interdipendenti tra di loro, più il sistema è esposto al rischio che si verifichino incidenti. In questo senso, alcuni sistemi inevitabilmente vedranno verificarsi degli incidenti più o meno gravi. Perrow inoltre, argomenta di come le commissioni incaricate di investigare su un dato incidente incorrano spesso in malintesi andando a ricercare le cause in un singolo individuo, una singola figura, un singolo componente del sistema quando, invece, come illustrato poc'anzi, un errore è il risultato di una serie di eventi concatenati e imprevedibili. Proprio in quanto gli incidenti e i guasti sono conseguenze dell'elevato grado di complessità dei moderni sistemi, l'unica soluzione al problema, suggerita dalla NAT e dal suo autore, è quella di ridurre il grado di complessità. Secondo Perrow il rischio di gravi incidenti, può essere evitato solamente diminuendo il grado di complessità e quindi in un certo senso distruggendo la tecnologia (l'esempio più calzante riportato dall'autore è quello delle centrali nucleari, la quale complessità può portare a disastri particolarmente gravi e, l'unico modo per azzerare il rischio di possibili catastrofi, è quello di abbandonare tale tecnologia).

[4] Incidente di Three Mile Island http://it.wikipedia.org/wiki/Incidente_di_Three_Mile_Island

Un altro gruppo di ricerca, studiando organizzazioni simili a quelle proposte da Perrow, è giunto a conclusioni molto simili. Nonostante queste organizzazioni affrontassero comunque il problema della complessità e delle numerose connessioni dei propri componenti, attraverso degli studi incentrati sulla sicurezza, sono state identificate realtà con elevati livelli di affidabilità e bassi livelli di rischio [17]. Queste organizzazioni, sono riuscite a creare un maggiore livello di sicurezza applicando particolari strategie. Queste possono essere riassunte come segue:

1) L'organizzazione è incentrata sul rischio e un'elevata formazione tecnica, unita ad un'elevata comunicazione dei dipendenti, permette all'organizzazione di essere reattiva qualora si presenti un problema più o meno grave.
2) Quando la complessità diventa difficilmente gestibile per un solo individuo, si attiva un sistema informale che mette in comunicazione varie componenti dell'organizzazione (come ad esempio specialisti tecnici, responsabili di settore, impiegati) in modo che ogni problema possa essere affrontato come se vi fosse un'unica mente collettiva in grado di affrontare la questione da ogni punto di vista e risolverlo nel migliore dei modi.
3) Effettuare backup periodici dei dati (ottenendo quindi una ridondanza dei dati).
4) La capacità di comprendere le complessità della tecnologia e dei processi produttivi anche attraverso gli errori e le esperienze passate.

Le quattro strategie appena descritte, caratterizzano le HRO (High Reliability Organizations).
La questione che per noi può essere rilevante è capire se, con la complessità creata tramite l'introduzione dell'Information and Communication Technology (ICT), si arriverà ad avere delle HRO o, se gli incidenti diventeranno la norma nei sistemi aziendali e bisogni di fatto arrendersi all'evidenza di dover correre perennemente dei rischi più o meno gravi.
La velocità del cambiamento, gioca un ruolo fondamentale nella gestione dei rischi; in quanto con riferimento ai sistemi complessi citati sopra, le nostre conoscenze riguardo le loro componenti e le loro interazioni, saranno sempre incomplete ai nostri occhi. Fin quando un sistema rimane stabile, con il passare del tempo si ha la possibilità di approfondire le proprie conoscenze riguardo il suo funzionamento ma, qualora avvenisse un cambiamento, – ad esempio l'introduzione di una nuova tecnologia – le conoscenze accumulate fino a quel momento dall'organizzazione, risulteranno insufficienti e/o incomplete. Con il passare del tempo, saremo nuovamente in grado di conoscere il nuovo sistema ma, solamente fintanto che

non avvenga un ulteriore cambiamento e così via. C'è da aggiungere che, più il sistema è complesso (in termini di numero di connessioni e di sue componenti), più risulterà lenta la fase di apprendimento. Se aumentasse la velocità del cambiamento, ad un certo punto il sistema si evolverebbe più rapidamente di quanto saremmo in grado di poterlo comprendere.
La fase dell'apprendimento, nelle organizzazioni, è stata studiata anche nell'ottica di una "miopia d'apprendimento". Levinthal e March (1993) [18], affermano che esistono tre tipi di miopia: una temporale, una spaziale e una fallimentare. Questo spiega come le organizzazioni (ed i membri che ne facciano parte) tendano a dimenticare facilmente eventi distanti in termini sia di spazio che di tempo (come ad esempio delle problematiche affrontate anni prima) e che questi tendano a sovrastimare i successi e a sottostimare gli insuccessi. La miopia dell'apprendimento è particolarmente rilevante nello sviluppo di soluzioni ICT perché "l'intelligenza aziendale" risulta spesso insufficiente nell'affrontare nuove problematiche e nuovi progetti di ICT. Questo problema è più evidente quando vi è un alto turnover di dipendenti nell'Information System Development (IDS).
Più un sistema diviene complesso e globalizzato, più difficile sarà notare la rilevanza di eventi distanti nel tempo e nello spazio ma, allo stesso modo, l'importanza di questi eventi aumenta con l'aumentare delle distanze.

2.2 TFI model. [2]

Molte definizioni sono state formulate per descrivere la sicurezza nelle aree di *Information Technology* (IT) e *Information System* (IS) e, l'*Information Security* (InfoSec) è un concetto d'uso comune, una più ampia accezione della sicurezza dei dati e dell'IT nel suo insieme. L'U.S. National Information Systems Security Glossary definisce l'Information System Security come: "la protezione di sistemi informativi contro accessi non autorizzati, inclusa la loro modifica, quando memorizzati o in transito e, contro la negazione del servizio ad utenti autorizzati o la prestazione di questo ad utenti non autorizzati, incluse tutte le misure necessarie ad individuare, documentare e contrastare tali minacce". In dottrina vengono evidenziate quattro caratteristiche fondamentali dell'Information Security: disponibilità, riservatezza, integrità, responsabilità.
Per disponibilità si intende il corretto uso delle risorse entro un lasso di tempo considerato idoneo.

La riservatezza consiste nel rendere leggibile l'informazione solamente agli attori della transazione.
L'integrità riguarda la protezione dei dati nei confronti di modifiche non autorizzate dovute a terze parti o ad eventi accidentali.
La responsabilità si riferisce alla capacità del sistema di responsabilizzare l'utente qualora compia una determinata azione.
Per ottenere queste quattro caratteristiche, sono richieste misure di sicurezza tecniche ed amministrative. La sicurezza amministrativa riguarda la gestione dell'IS Security, come la scelta delle strategie da adottare, le politiche di sicurezza, l'analisi dei rischi, la formazione del personale ecc. Questo lato dell'IS Security, è da intendersi ad un livello organizzativo considerando l'insieme azienda come unica entità. La sicurezza tecnica invece, riguarda tutte quelle misure da adottare al fine di proteggere le infrastrutture e può essere divisa in sicurezza fisica e sicurezza IT. La sicurezza fisica sta ad indicare la protezione delle apparecchiature tecnologiche in senso stretto, come ad esempio la protezione da eventi come incendi, allagamenti ecc. La sicurezza IT invece, si riferisce alla sicurezza delle informazioni in un sistema informativo in senso tecnico e può essere ulteriormente suddiviso in sicurezza dei computer e sicurezza delle comunicazioni. La prima si riferisce alla protezione dell'hardware e i suoi componenti, come tecniche di criptazione e di backup dei dati. La seconda invece, è da intendersi come la gestione dei network e degli altri media che regolano il flusso dei dati all'interno degli stessi, come ad esempio i firewall.
Il modello descritto finora però, non chiarisce come sia composto il livello della sicurezza amministrativa e, alcune ricerche sul tema, hanno dimostrato come sia necessaria un'implementazione di questo.
Una soluzione a tale problema è stata proposta tramite l'estensione il modello dando però maggior peso agli standard di sicurezza internazionali, ai metodi e i modelli adottati in realtà differenti.
Per introdurre l'estensione del TFI model, possiamo affermare che un sistema informativo sia costituito sostanzialmente da tre parti; una tecnica, una formale e una informale. Possiamo inoltre affermare che la gestione informale delle informazioni in un'organizzazione è fondamentale e non sempre può essere sostituita da regole proprie di un sistema tecnico. Adottando questa visione degli elementi informali (come la percezione del rischio da parte dei dipendenti, la consapevolezza dell'ambiente in cui si opera, i desideri di ciascuno di loro, la cultura propria, ecc.), bisogna tenere in considerazione che questa è fortemente correlata con

il contesto in cui opera e, che questa dovrebbe guidare l'impostazione delle soluzioni formali (politiche di sicurezza, processi di business, standard adottati, procedure ecc.) e tecniche (come le piattaforme software e hardware adottate, l'infrastruttura del network, i dispositivi utilizzati ecc.). Volendo fare ora un focus più approfondito sugli elementi del TFI model (Technical, Formal e Informal), passiamo a chiarire gli aspetti caratterizzanti di ognuno dei tre elementi appena introdotti.

Livello di sicurezza Tecnico. Da un punto di vista tecnico, la preservazione della riservatezza, integrità, disponibilità e responsabilità, richiede l'adozione di soluzioni tecnologiche come: la criptazione dei dati e delle comunicazioni, intercettazioni fisiche, un sistema di controllo degli accessi, meccanismi di autenticazione e autorizzazione ecc. A questo livello è possibile far uso di modelli e metodi per la scelta delle migliori soluzioni tecnologiche da adottare.

Livello di sicurezza Formale. Il livello formale è collegato a tutto l'insieme delle norme, delle regole, dei controlli, degli standard adottati ecc., al fine di definire un'interfaccia intermedia posizionata tra il sottoinsieme tecnologico (livello tecnico) e quello comportamentale (livello informale). Questo può essere indicato come il livello dove la maggior parte dello sforzo dell'Information Security management è concentrato.

Livello di sicurezza informale. Nell'ambito del livello informale della sicurezza IS, l'analisi viene svolta sugli individui e la ricerca è concentrata sui problemi comportamentali come valori morali, attitudini personali, credenze e, tutte le norme che possono influenzare il comportamento degli individui comprese le pratiche di sicurezza nelle organizzazioni.

Questo approccio risulta utile nella gestione delle minacce interne. Numerosi studi hanno evidenziato come sussistano dei problemi nella gestione della sicurezza informativa, specialmente del controllo del comportamento umano degli individui. Alcuni studi hanno inoltre messo in evidenza come molte volte gli impiegati aggirino tali misure di sicurezza interne al fine di ottenere determinati vantaggi essenzialmente perché esiste la possibilità di farlo. Il problema diventa di maggior rilievo qualora l'azienda sia geograficamente dispersa, il che rende difficile l'implementazione di misure di sicurezza adeguate.

Tali misure di livello informale, comprendono anche interventi contro attacchi di ingegneria sociale[5]. Gli hacker traggono vantaggio da possibili falle nella sicurezza e, questo nuovo tipo di ingegneria fa leva proprio su uno degli aspetti meno sicuri che vi siano; la psiche umana. L'ingegneria sociale trae origine dalla psicologia ed è utilizzata dagli hacker per riuscire ad ottenere quelle informazioni che teoricamente non dovrebbero possedere. Con tali

5 Ingegneria sociale http://it.wikipedia.org/wiki/Ingegneria_sociale

informazioni si intendono password, user ID e tutti gli altri tipi di informazioni sensibili. Le barriere tecniche costruite tramite i paradigmi tecnici e formali non sono così sufficienti a contrastare tale fenomeno.

Un modo per estendere il modello InfoSec visto in precedenza, è quello di ampliare il lato amministrativo utilizzando gli elementi formali e informali del TFI model. La sicurezza amministrativa riguarda la gestione della sicurezza informatica, dove vi si presentano gli elementi formali e informali. Secondo quanto detto in precedenza, gli elementi formali includono le politiche di sicurezza, le regole di controllo, gli standard ecc., tutto ciò che serve a definire un'interfaccia tra il sistema tecnico e quello informale, che include gli aspetti legati ai comportamenti umani. Con riguardo al lato formale, sembra necessario suddividerlo ulteriormente nei livelli "esterni" ed "interni". Ogni organizzazione infatti, è soggetta a una regolamentazione esterna riguardante i problemi di sicurezza come ad esempio le leggi sulla sicurezza sul lavoro, regolamenti e vari accordi stipulati con altre società ed organizzazioni intra aziendali. Inoltre, esiste un formalismo interno che riguarda la gestione della sicurezza informativa, come strategie di IT, politiche di sicurezza, corsi d'aggiornamento per i dipendenti.
L'estensione del modello InfoSec, generato grazie al *TFI model* può essere schematizzata come segue.

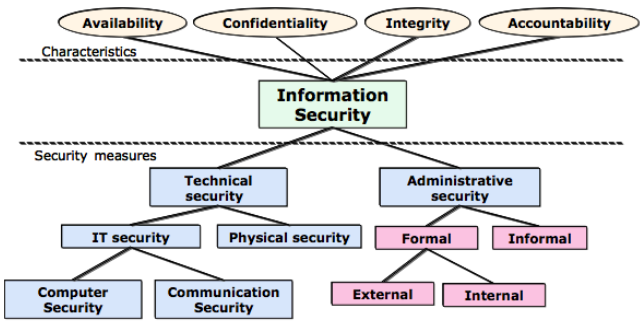

Figura 2.1 Modello InfoSec esteso [2]

2.3 Bilanciamento strategico tra prevenzione e risposta. [1]

La gestione della sicurezza nei sistemi informativi è senza dubbio un'attività critica in un mondo dove l'informatica è onnipresente e i sistemi interconnessi tra di loro. Con il passare del tempo, sono stati formulati numerosi standard internazionali nella gestione della sicurezza di tali sistemi, alcuni di questi sono proprio quelli visti in precedenza (ISO, COBIT e PCI). Questi prescrivono l'uso di particolari contromisure tecniche, formali ed informali. Storicamente i vari standard, si sono concentrati molto su un controllo da effettuare "a priori", ponendo l'accento sulla qualità del sistema e sulle sue performance. I più recenti approcci di gestione della sicurezza invece, semplicemente selezionano i controlli da checklists dove, successivamente, tramite un approccio più sofisticato, si misura l'esposizione al rischio del sistema. Come risultato, si può notare che l'attenzione è posta maggiormente sulla prevenzione di possibili danni noti. Questa filosofia orientata alla prevenzione, con il suo set di controlli predefiniti, però, mal si concilia con un mondo sempre più dinamico, dove l'esposizione al rischio aumenta all'aumentare della grandezza aziendale. Con l'avanzare del tempo e il progredire della tecnologia, gli hacker hanno cominciato ad utilizzare attacchi sempre più di tipo dinamico, scovando quelle mancanze presenti nelle filiere di controllo, tipiche delle organizzazioni e riuscendo così a bypassare gli enormi investimenti che vengono approvati ogni anno da numerose aziende in tutto il mondo. Celebri sono i casi di Stuxnet[6] e Aurora[7]. L'aumentare di ambienti a sicurezza dinamica, richiede però, misure di sicurezza maggiormente orientate sulla risposta a tali eventi. Vi è così la necessità di passare da una visione incentrata sulla prevenzione ad un più ampio quadro di gestione della sicurezza informatica. Questo, si focalizza sul bilanciamento tra prevenzione e risposta attraverso un punto in comune, rappresentato dall'incidente. Immaginando una linea temporale dell'incidente, la "prevention" agisce prima di tale evento, mentre il "response" successivamente (si veda la figura 2.2).

Esistono inoltre, profonde differenze tra la gestione di strategie di prevenzione e di risposta. Queste, derivano dalle definizioni contrastanti di affidabilità e validità. Una predizione si dice affidabile quando si è rivelata corretta in passato mentre una predizione è valida quando risulta corretta nel presente. L'affidabilità è quindi ancorata al passato mentre la validità al futuro. Possiamo pertanto affermare che il termine "prevention" si riferisce a quei principi e

6 Stuxnet http://it.wikipedia.org/wiki/Stuxnet

7 Operazione Aurora http://it.wikipedia.org/wiki/Operazione_Aurora

quelle pratiche proprie dei sistemi di sicurezza informatica presenti nelle organizzazioni che hanno lo scopo di prevenire il verificarsi di un incidente. Il termine "response" invece, si riferisce a quei principi e quelle pratiche proprie delle organizzazioni, dove si ha l'intento di reagire agli incidenti.
Questi due paradigmi sono tanto indipendenti quanto complementari e, rappresentano due strategie di gestione della sicurezza differenti tra di loro.
Per quanto riguarda la gestione della sicurezza, i manager dovrebbero porsi il problema di bilanciare correttamente le strategie, scegliendo di dare maggior peso all'uno o all'altro paradigma, tenendo però in considerazione il contesto d'operatività dell'azienda. Le organizzazioni dovrebbero inoltre rivedere il proprio bilanciamento tra i due paradigmi qualora il contesto organizzativo cambiasse, ad esempio, diventando maggiormente dinamico il rischio di minacce crescerebbe.

Possiamo ora fornire una definizione formale di incidente in un sistema informatico e definirlo come: "un cambiamento di stato di un determinato sistema informatico, il quale muta da uno stato desiderato ad uno indesiderato e, dove il cambiamento è dovuto all'uso di stimoli esterni al sistema" [19]. In altre parole, il momento dell'incidente rappresenta un evento che aggira ogni controllo preventivo e vi infligge cambiamenti negativi.
Rispettando questo punto di vista, possiamo affermare che il momento dell'incidente è il fulcro dell'idea "prevenzione vs risposta". Questo segna il passaggio dal momento in cui il sistema era protetto – grazie alla prevenzione – a quando invece viene modificato essendo stato violato. Se una minaccia era conosciuta in passato, possono applicarsi i principi di affidabilità e sfruttamento, propri della prevenzione, nella gestione del processo di difesa contro tale minaccia.
Il paradigma della prevenzione può quindi posizionarsi sul lato sinistro di una ideale timeline, dove al centro è posto l'evento incidente. Se la minaccia era sconosciuta in passato, invece, vanno applicati i principi di validità ed esplorazione, al fine di gestire al meglio la risposta contro il danno. Il paradigma risposta può quindi essere posizionato sul lato destro della medesima timeline. Come mostrato in figura 2.2.
Organizzazioni operanti in ambienti stabili e, dove la tecnologia non muta rapidamente, sicuramente opteranno per l'adozione di una strategia più orientata alla prevenzione, dove le possibili minacce sono ben note ed è richiesto un elevato grado di controllo. Viceversa, quelle organizzazioni il cui business è posizionato in settori di mercato maggiormente dinamici,

adotteranno strategie volte alla risposta; proprio in quanto le minacce sono mutevoli e mutevoli devono essere anche le misure di sicurezza.

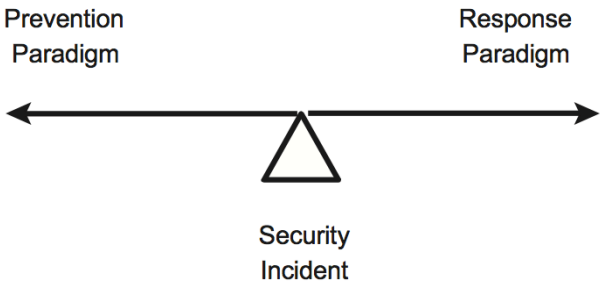

Figura 2.2 Bilanciamento strategico tra prevenzione e risposta. [1]

Bisogna inoltre sottolineare che, qualora si puntasse maggiormente ad un approccio di risposta, questo non significherebbe che debba essere abbandonata ogni forma di prevenzione, come ad esempio l'uso di password nell'accesso ai sistemi informatici.

Il modello della prevenzione, opera guardando attraverso le esperienze passate dove le minacce sono conosciute, dando la così possibilità di prevedere l'accadimento di eventi simili in futuro.

Per prevenire il verificarsi di un tale evento, è innanzitutto necessario sviluppare evidenze riguardo agli avvenimenti passati. La prevenzione evoca predizione, previsione o stime sulla natura e verosimiglianza di un dato evento, basandosi su incidenti precedenti. Uno degli strumenti fondamentali pertanto è l'analisi del rischio, la quale fornisce le probabilità che un particolare evento possa accadere, i costi e le perdite ad esso associate. Il modello di risposta invece, implica la pianificazione di azioni che accadranno in futuro. Il migliore esempio del paradigma di risposta è il disaster recovery plan o il business continuity plan.

Il modello della risposta incorpora la preparazione a minacce sconosciute, inaspettate o imprevedibili e, una caratteristica fondamentale del "response" è l'agilità con cui questo entra in gioco.

Volendo ora fare un focus più dettagliato sulle assunzioni fondamentali che stanno alla base dei due paradigmi, possiamo affermare che il prevention paradigm implica che:

1) I rischi siano prevedibili.
2) I rischi siano misurabili.
3) I rischi siano persistenti.

4) Che sussista una relazione statica tra rischio e salvaguardia. La relazione tra rischi e salvaguardia è quindi ben definita a priori. Le analisi di sicurezza determinano le metodologie di protezione, le quali provvedono ad instaurare nel concreto, delle misure difensive.
5) Una logica di prevenzione. La teoria della varianza è alla base della logica fondante l'approccio di prevenzione. Questa assume una relazione causale tra variabili predittive e dipendenti. Secondo questa teoria, il livello della variabile predittiva può determinare il risultato di una variabile dipendente. Esempi sono: "se X allora Y" oppure, "se più X allora più Y".
6) Apprendimento a ciclo unico. Questa modalità d'apprendimento implica che, i problemi e le relative soluzioni, siano vicini tra di loro in termini di spazio e tempo. Piccoli cambiamenti sono apportati da specifiche procedure, basate su ciò che ha funzionato o che non ha funzionato in passato. Questo processo, implica il migliorare le cose, senza però modificare o eliminare le assunzioni e la filosofia che ne stanno alla base. L'apprendimento a ciclo unico porta a compiere minori correzioni, come ad esempio piccole modifiche di una configurazione firewall nel controllo dell'accesso al network.

Considerando invece, il response paradigm, assumiamo che:

1) I rischi siano imprevedibili. Esempi di rischi imprevedibili sono gli attacchi 2.0, gli APT[8] e i rischi dinamici descritti in precedenza.
2) I rischi non siano misurabili. Non possono essere misurati in quanto sono imprevedibili.
3) I rischi siano transitori. Questo significa che gli attacchi sono innovativi e inaspettati, al fine di cogliere impreparate le difese.
4) Che sussista una relazione dinamica tra rischio e salvaguardia. Le organizzazioni dovrebbero rispondere ai nuovi rischi sviluppando velocemente delle difese personalizzate. La relazione tra rischio e salvaguardia, non è solo dinamica ma anche consequenziale. Alla base vi è un agile processo di messa in sicurezza, dove vengono sviluppate misure di difesa innovative e persistenti.
5) Una logica di risposta. la logica fondante del response paradigm è la teoria di processo. Questa non assume una relazione causale tra le variabili predittive e quelle dipendenti. Si assume che quella predittiva sia insufficiente ma necessaria a fornire l'output. La forma logica della teoria di processo è " se no X allora no Y" ma questo non implica che "se più X allora più Y".
6) Apprendimento a ciclo doppio. Questo assume che le organizzazioni devono esaminare e modificare le proprie assunzioni e le loro ipotesi di base al fine di trovare una soluzione al problema. L'apprendimento a ciclo doppio è rilevante quando si devono prendere importanti decisioni dove, solitamente accade che vengano modificate le variabili, le politiche, la governance.

La figura 2.3, fornisce una visione d'insieme su quanto è stato detto finora. Il momento dell'incidente è situato al centro della figura, il momento precedente è situato alla sinistra del

[8] Advanced persistent threat http://en.wikipedia.org/wiki/Advanced_persistent_threat

"bang" mentre il momento successivo, alla sua destra. La parte sinistra è dominata dal prevention paradigm mentre quella destra dal response paradigm. Entrambe sono connesse in una visione proattiva e una reattiva. La parte sinistra dell'incidente (prevention paradigm) è maggiormente proattiva, nel senso di poter prevedere i rischi misurabili così da prevenirli tramite appositi sistemi difensivi. Il prevention paradigm, quindi si focalizza sul ridurre futuri attacchi indirizzati verso le debolezze già conosciute.

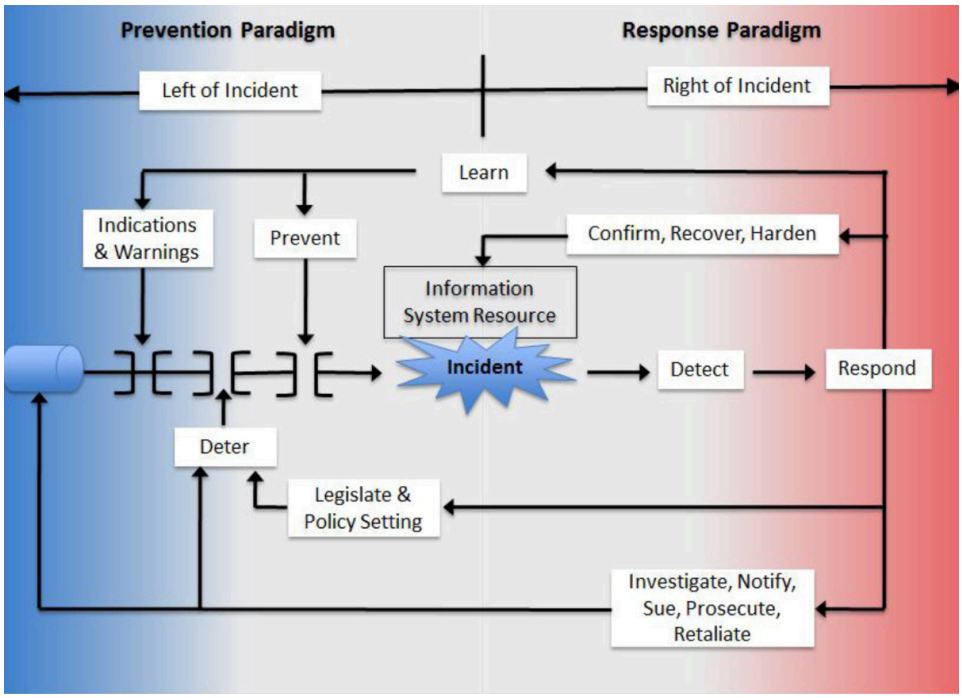

Figura 2.3 Interazione del paradigma di prevenzione e risposta. [1]

Al contrario invece, sul lato destro dell'incidente, il response paradigm è maggiormente reattivo nello scovare quelle violazioni imprevedibili e inaspettate, riuscendo così a rispondervi. Focalizzandoci sugli attacchi prevedibili, il response paradigm cerca di individuare le perdite reagendo velocemente ed efficientemente nel riprendersi dall'attacco.
Avendo effettuato questa analisi sui due paradigmi, possiamo quindi affermare che il prevention paradigm è tipicamente dominante nelle organizzazioni commerciali. Un ambiente stabilmente sicuro dove le risorse sono prontamente disponibili e gli attacchi che vengono effettuati sono persistenti e prevedibili. Possiamo anche affermare che invece, il response paradigm è tipicamente dominante nelle organizzazioni militari. Un ambiente instabile e

insicuro dove le risorse sono contenute e gli attacchi non sono ne persistenti e ne prevedibili. Ovviamente non tutte le organizzazioni commerciali e non tutte quelle militari operano in tali ambienti.

Avendo così esposto le principali teorie sull'argomento, nel prossimo capitolo verranno applicati tali modelli nell'analisi di nove dei più eclatanti casi ripostati in appendice. L'intento sarà quello di fornire evidenze empiriche su quanto è stato teorizzato in questo capitolo.

3. Analisi dei casi.

3.1 Metodi e finalità di ricerca

In questo capitolo verranno analizzati nove casi di studio dove, delle aziende hanno subito un attacco informatico più o meno grave. Basandoci sulle teorie esposte nel capitolo precedente, condurremo un'analisi empirica su tali casi, sul come e sul perché queste società abbiano adottato tali impostazioni di prevenzione e risposta e di come sia strutturata l'organizzazione sotto il profilo del TFI model. Lo scopo della ricerca è quello di confermare in modo empirico quanto teorizzato precedentemente e speculare su quali potrebbero essere gli assetti più consoni da adottare in futuro data la natura della società, il livello di complessità tecnologico aziendale e la posizione di mercato occupata. A tal proposito, in ultima istanza verrà proposta un'analisi cross dimensionale dove verranno adottati dei termini di paragone capaci di comparare i vari casi e scovare differenze e similitudini su quale sia il loro bilanciamento tra prevenzione e risposta date le relazioni di rischio e salvaguardia, considerando quindi anche la tipologia di rischi assunti.

Avendo scelto, per la conduzione della ricerca, società operanti soprattutto all'estero (nella maggior parte dei casi negli Stati Uniti) ed essendo queste, società di grandi dimensioni, influenti nei rispettivi segmenti di mercato, non è stato possibile condurre interviste dirette con i rispettivi security manager. Si è però fatto affidamento su documenti ufficiali, documenti di ricerca a fini didattici e non, su articoli pubblicati da autorevoli riviste scientifiche quali ad esempio la Elsevier e su articoli di cronaca di famose testate giornalistiche come Forbes o Reuters. Tutti i documenti saranno citati in bibliografia.

Va inoltre precisato che tutti gli elementi bibliografici saranno esplicitati nella relativa scheda del caso consultabile in appendice.

3.2 Caso uno: TJX Companies, Inc.

TJX Companies è una società Americana che si occupa di abbigliamento e prodotti per la casa con sede in Framingham, Massachusetts. Sostiene di essere la più grande compagnia di abbigliamento e prodotti per la casa degli Stati Uniti.

Come ipotizzato in teoria, per un'azienda come TJX, che si occupa principalmente della vendita di beni di consumo, il bilanciamento tra prevenzione e risposta dovrebbe tenderne verso il primo. Colui che si occupa dell'implementazione, della gestione e della messa in sicurezza di tutta l'infrastruttura IT è il Chief Information Security Officer (CISO). Nel nostro caso, la sua più grande responsabilità è sicuramente quella di riuscire ad implementare al meglio le nuove strutture IT con l'intera infrastruttura aziendale, tenendo presente che debba considerare anche l'esistenza di una precedente struttura informatica e quindi il dover far cooperare al meglio le più nuove tecnologie con quelle più datate. Compito sicuramente non semplice dato il core business aziendale e il dover far fronte a problematiche quali ad esempio, la contingenza del budget – che, nel nostro caso è stata la causa scatenante con la quale gli hacker sono riusciti a superare le misure di sicurezza -, il dover far cooperare più tecnologie insieme, il dover formare i dipendenti riguardo l'uso delle nuove strumentazioni, l'efficiente allocazione delle risorse e il dover prioritizzare i problemi attraverso un'analisi del rischio. Data la posizione di mercato occupata, potremo affermare che in questo caso, la prevenzione è dominante nel core delle strategie IT in quanto i rischi sono percepiti come prevedibili ed è possibile farne un'analisi qualitativa e quantitativa. Oltre ciò, potremo affermare che per TJX, i rischi sono misurabili e persistenti, data la considerazione che sussista una relazione statica tra rischi e salvaguardia.

In questo contesto, la protezione della disponibilità, integrità e riservatezza dei dati è sicuramente un tema di rilievo, in quanto le informazioni devono essere sempre disponibili al fine di evitare disagi nella gestione dell'intera azienda (si pensi ad esempio, quando viene effettuato un acquisto, i dati della merce devono essere disponibili, altrimenti si andrebbe incontro a gravi problematiche, quali ad esempio la cattiva gestione del magazzino). I dati devono essere anche integri, in quanto se ciò non fosse, si andrebbe incontro a problemi simili a quelli visti per la mancanza di disponibilità. Ancor più rilevante, però, i dati devono essere confidenziali. Questo è un punto chiave in quanto la società non solo immagazzina dati

relativi alla propria attività, ma anche un'enorme quantità di dati relativa ai propri clienti. La perdita di riservatezza pertanto, rappresenta un problema cardine, in quanto oltre ai danni diretti verso la società, una fuoriuscita di questo tipo di informazioni, rappresenterebbe un problema di ordine pubblico. Questo però è quanto successe a TJX; la perdita di riservatezza.
Nel 2005, un gruppo di hacker, sfruttando delle debolezze della rete di sicurezza WLAN, riuscirono ad intercettare i dati in transito in alcuni negozi di TJX. Gli hacker si erano posizionati fuori dai negozi (in particolare quello di Marshall in St. Paul, Minnesota) e con una particolare antenna, per due giorni consecutivi, sono riusciti a catturare l'intero traffico in transito nel wireless network dello store, assicurandosi che nessuno avesse notato nulla. Dopo ciò, con i dati in loro possesso riuscirono a rompere il codice di sicurezza WEP del negozio riuscendo così ad avere accesso ad un gran numero di dati, tra cui tutte le transazioni effettuate e i relativi dati delle carte di credito utilizzate per i pagamenti. Successivamente, nella seconda metà del 2006, i criminali riuscirono ad arrivare ai database principali ottenendo così, oltre che delle informazioni vitali per l'azienda, anche un'enorme mole di dati sui clienti. Si pensa che siano più di 45 milioni i dati rubati. Come da quanto appena descritto, la struttura di sicurezza della società, al momento della prima aggressione era molto debole. Venivano usati sistemi di cifratura obsoleti (quali era il sistema Wired Equivalent Privacy WEP) e ciò ha fatto sì che gli intrusi, una volta appreso il metodo di sicurezza utilizzato, non impiegassero molto ad invadere la rete.
Questo mette in luce quanto descritto sopra e quanto nella teoria. TJX, dovendo assegnare delle priorità ai possibili attacchi che sarebbero potuti avvenire, ha preferito rimandare l'aggiornamento delle infrastrutture di comunicazione wireless, lasciando così libera strada a possibili avventori nello sfruttare tale debolezza. Quando è stato deciso di rimandare tale aggiornamento, evidentemente non era stata assegnata la giusta priorità al rischio. Ne tantomeno il CISO ha fatto pressioni sulla direzione per far approvare l'upgrade, nonostante fosse a conoscenza del fatto che, altre organizzazioni prima di loro, avessero subito intrusioni simili tramite quella particolare falla di sicurezza. Questo mette in risalto come il response paradigm (che si sarebbe dovuto attivare già tramite il double loop learning nell'osservazione delle altre aziende bersaglio di attacchi simili) non fosse particolarmente sviluppato (ciò è giustificato dal fatto che TJX opera in un settore di mercato dove solitamente si da maggior peso ad una prevenzione di tipo statico). Ciò si mette in linea con quanto teorizzato riguardo il bilanciamento tra prevenzione e risposta. Una volta che l'attacco fu portato a termine e che fu compreso come gli hacker fossero riusciti ad invadere il network, si è comunque attivato il

paradigma di risposta. Il management decise di adottare immediatamente il più sicuro protocollo di sicurezza WPA (Wifi Protected Access) e successivamente dare il via alle indagini. Dopo aver appreso l'entità del danno, si è deciso di avvertire la law enforcement agency e, solamente qualche tempo dopo, il 17 gennaio 2007 è stata resa pubblica la notizia. Questa ha portato ad ulteriori indagini esterne riguardo l'accaduto, i quali hanno messo in luce ulteriori problemi di sicurezza, successivamente risolti.
Cercheremo ora di individuare, tramite il modello del thecnical, formal, e informal (TFI model) quali aree abbiano permesso tale l'intrusione. Sicuramente l'area meno strutturata sotto questo punto di vista era quella tecnica. L'area della Technical security che ha fatto sì che si perdesse la riservatezza dei dati è quella della Communication Security (vedi Fig. 1, capitolo 2). Come sopra citato, le misure di sicurezza adottate erano obsolete e, nonostante il CIO Paul Butka avesse già menzionato questo handicap e suggerito l'adozione di standard più sicuri (quali quello WPA), si è preferito evitare ulteriori costi e rimandare l'aggiornamento ad una data futura esponendo così la società al rischio che poi ha effettivamente corso. Anche l'area formale della sicurezza amministrativa evidenziava carenze. Infatti, bisogna sottolineare che già nel 2005 la compagnia non rispettava 9 dei 12 requisiti di sicurezza imposti dai nuovi standard PCI DSS e nonostante ciò, la società non si mise in linea con tali standard fintanto che non si verificò l'incidente. Per quanto riguarda l'area informale della sicurezza amministrativa invece, non risulta essere in alcun modo responsabile del furto dei dati messo in atto. Ovviamente non possiamo affermare con certezza che al tempo la società fosse in linea con i migliori criteri di sicurezza informale, in quanto non avendo intervistato direttamente i responsabili aziendali, non siamo in gradi di poterci esprimere. In ultima analisi, con quanto sopra riportato, sembra che in questo caso, la realtà abbia confermato quanto teorizzato nel capitolo precedente.

3.3 Caso due: Target Corporation.

Target Corporation è una società di vendita al dettaglio americana, fondata nel 1902 e con sede in Minneapolis, Minnesota. Con più di 366.000 dipendenti è la seconda società di questo genere negli Stati Uniti (Walmart è la prima). Come TJX, anche Target è una società di vendita al dettaglio con un vasto catalogo di prodotti ben diversificato e con un'area di mercato molto simile. La struttura organizzativa e societaria sembra quindi essere

pressappoco la stessa, dove ad esempio la figura dirigenziale più influente non è di certo il CISO, il quale svolge un ruolo di supporto all'intera organizzazione, in quanto l'IS e l'IT più in generale, non è certamente nel core business della società. Questo comporta che, come nel caso di TJX, vengano assegnate priorità maggiori a progetti differenti dalle implementazioni informatiche, dagli adattamenti tecnologici o da adozioni di nuove strumentazioni più sofisticate. Questo ovviamente non sta a significare che la società (o tutte le altre presenti nel medesimo settore di mercato) non diano il giusto peso ai progetti informatici, anzi. Data la crescita esponenziale della tecnologia e dell'uso che ne si fa – basti pensare ad internet -, anche aziende distanti da questo mondo ne fanno sempre più uso, sia come supporto nella gestione delle funzioni organizzative, sia nell'operatività aziendale, sia come strumento di comunicazione. Nel nostro caso, Target ad esempio, possiede un vasto sito internet dove gli utenti possono agevolmente acquistare qualsiasi prodotto anche da casa. Forte è anche la sua presenza sui social media, con la quale comunica con la clientela, fornisce sempre gli ultimi aggiornamenti in tempo reale e, cerca di aumentare il proprio parco clienti – ad esempio tramite l'utilizzo di inserzioni sui principali social media -. Nonostante questa forte presenza sul web, il core business aziendale rimane impiantato sulla vendita di beni di consumo tramite i propri negozi fisici e, di conseguenza anche il bilanciamento tra prevenzione e risposta risulta maggiormente orientato verso il primo.

Potremmo fare sicuramente considerazioni molto simili con il caso precedente anche per quanto riguarda l'importanza della perdita di riservatezza, integrità e disponibilità dei dati. Come in TJX, nel malaugurato caso che i dati non dovessero essere disponibili o integri, si verrebbero a creare situazioni potenzialmente molto spiacevoli, in quanto anche in questo caso potrebbero venire ad esistenza problematiche riguardanti ad esempio, il processo della gestione di un ordinativo. La riservatezza dei dati, come abbiamo visto, è un aspetto sicuramente di maggior rilievo in una realtà di questo genere. Dal momento che Target (e la gran parte delle altre aziende operanti nel medesimo settore) registra e archivia ogni transazione, una eventuale fuoriuscita di dati creerebbe numerosi problemi, sia di natura economico-finanziaria che di reputazione del nome aziendale (probabilmente questo è l'aspetto preponderante quando si vanno a conteggiare i costi relativi ad un evento simile. Si pensi ad esempio al corro di valore che subirebbero i titoli azionari della società). Quando vengono compiute delle transazioni (sia tramite i rivenditori fisici che quelli online) i dati relativi alla clientela vengono memorizzati su database appositi. Questo fa si che la rilevanza dei dati in possesso cresca col crescere del proprio parco clienti, in quanto vengono

memorizzati, oltre che dati di accesso al sito internet o i nominativi della clientela (ad esempio quando viene richiesta una fattura), anche i dati delle carte di credito, qualora si utilizzasse tale metodo di pagamento. Questa grandissima mole di dati posseduti da questo tipo di società, può incentivare attività criminose con il fine di entrare in possesso di tali dati, sfruttando anche la considerazione che, dato il core business aziendale, l'infrastruttura tecnologica sarà qualitativamente inferiore a società in cui la tecnologia è un punto cardine dei loro servizi. Focalizzandoci su Target, possiamo notare come la dirigenza abbia investito molto sulla sicurezza IT ma, nonostante ciò, anche se attraverso una metodologia bizzarra, gli hacker sono comunque riusciti ad entrare in possesso dei dati da loro cercati. Gli hacker sono riusciti ad ottenere l'accesso ai database e quindi ai dati sensibili, attraverso più fasi. Dapprima hanno ottenuto informazioni (attraverso Google) circa il modo in cui Target si relazionava con i propri fornitori. Successivamente attraverso un particolare documento reso pubblico da Microsoft, sono venuti a conoscenza circa l'infrastruttura tecnica della società, inclusi importanti dettagli sul funzionamento dei POS (Point Of Sale). Dopo aver studiato nel dettaglio il funzionamento della tecnologia adottata, due mesi prima dell'attacco vero e proprio, venne inviata ad un fornitore di Target, un'email contenente un particolare malware in grado di creare un collegamento tra il sistema informatico del fornitore e quello di Target. Creato questo collegamento, per gli hacker non fu difficile infiltrarsi nel network di Target. Una volta entrati nel sistema riuscirono poi ad ottenere l'accesso al sistema che gestiva i POS istallando un ulteriore malware (capace di non essere identificato dagli antivirus) che si diffuse velocemente su tutti i dispositivi dei vari negozi. Il software istallato, era capace di memorizzare i dati delle carte di credito ogni qualvolta queste venivano strisciate sulla macchina e, attraverso un particolare canale di comunicazione creato appositamente per questo attacco, i dati venivano inviati agli intrusi rendendoli capaci di leggere in chiaro le informazioni appena rubate. Sotto l'aspetto della prevenzione questo caso risulta emblematico. Nonostante tutte le misure di sicurezza adottate (come ad esempio la conformità alle normative di sicurezza intra aziendali relative alla gestione dei POS) e la grande attenzione posta ai dati maggiormente sensibili, gli hacker sono comunque riusciti a penetrare all'interno del sistema. Anzitutto vi erano lacune di sicurezza nel momento in cui Target veniva in contatto con i propri fornitori utilizzando il sistema telematico. Questo deriva dal fatto che, i responsabili della sicurezza, al momento della progettazione dell'infrastruttura IT, hanno preferito porre maggiore attenzione ai dati direttamente archiviati nei database e non tanto sul sistema di comunicazione con i terzi. Questa mancanza ha fatto sì che non fosse

difficile per gli hacker penetrare nel sistema sfruttando proprio quei canali di comunicazione utilizzati per i rapporti con i loro fornitori. Altra importante lacuna è stata identificata nel sistema di gestione della sicurezza dei POS. Gli hacker sono riusciti ad istallare un malware all'interno dei dispositivi, in modo totalmente indisturbato e, riuscendo a farlo funzionare in modo tale che questi registrassero ed inviassero i dati appena acquisiti. Questo non doveva accadere. Si sarebbero dovuti utilizzare metodi più efficaci, quali ad esempio un sistema di whitelisting, il quale avrebbe permesso l'istallazione e l'esecuzione dei soli programmi contenuti. Effettuate tutte le indagini di dovere, collaborando sia con le autorità federali che con società private, Target ha provveduto immediatamente ad aggiornare le proprie misure di sicurezza, assicurandosi che un tale incidente non possa più verificarsi in futuro. Questo evento inoltre, ha anche fatto luce su evidenti problematiche proprie degli standard internazionali utilizzati per la messa in sicurezza delle infrastrutture tecnologiche ed in particolar modo per la protezione dei dati in transito sui dispositivi POS.

Passando ad analizzare l'incidente dal punto di vista del TFI model, possiamo affermare che tutte e tre le macro aree del modello avevano più di una lacuna. I problemi di sicurezza non erano solamente legati ad aspetti software, ben sì anche hardware. Si sarebbe potuto evitare l'accaduto adottando soluzioni come l'Hardware Security Module (HSM), il quale avrebbe assicurato l'istallazione di soli moduli dotati di un particolare codice, riconoscibile dal terminale, in modo che non sarebbe stato possibile istallare apparecchiature non conosciute. Ulteriori sistemi (come il Tamper Resistant Security Module, TRSM) si sarebbero potuti implementare in modo da proteggere il POS operating system memory che avrebbe evitato di memorizzare i dati criptati in versione software all'interno del POS, bensì in un apposito terminale hardware completamente indipendente. Ancora, si sarebbero potute utilizzare metodologie di supporto, come il Point-to-Point Encryption (P2PE), il quale avrebbe aggiunto un'ulteriore grado di sicurezza. Dal punto di vista formale, nonostante Target fosse in regola con quanto imposto dagli accordi di sicurezza intra aziendali, soffriva evidentemente in più di qualche punto nell'adozione di politiche di sicurezza interne. Sul lato informale del modello spiccano carenze di sicurezza laddove entri in gioco il comportamento umano. Dati i documento in nostro possesso, possiamo attribuire la colpa dell'accaduto all'azienda fornitrice di Target, Fazio Mechanical, la quale non avendo adottato la normale diligenza nel verificare la fonte dell'email portatrice del malware, ha fatto si che gli hacker potessero procedere con l'attacco. Probabilmente se i dipendenti fossero stati maggiormente informati sui possibili pericoli legati a email provenienti da fonti sconosciute, si sarebbe potuto evitare

un tale disastro. Come nel caso precedente, data la posizione di mercato occupata, la struttura organizzativa e i dati trattati, sembra che anche questo caso rispecchi quando teorizzato precedentemente.

3.4 Caso tre: Home Depot, Inc.

Home Depot è un venditore al dettaglio statunitense di prodotti per migliorare, costruire e manutenere la casa. Ha la sua sede a Vinings, nella Contea di Cobb (Georgia) appena fuori da Atlanta. Home Depot impiega più di 355.000 persone e gestisce 2.164 Superstore distribuiti negli Stati Uniti, Canada, Messico e Cina. Attualmente è il più grande distributore di prodotti per la casa degli Stati Uniti, davanti al rivale Lowe's, e il secondo più grande distributore in generale degli Stati Uniti, preceduto solo da Walmart. Come le altre due aziende appena analizzate, anche Home Depot è una società di vendita al dettaglio con un vastissimo assortimento di prodotti e un altrettanto vasto parco clienti. Nonostante i prodotti commercializzati possano essere in qualche modo diversi, non sussistono grosse differenze sul piano dell'organizzazione societaria e delle infrastrutture tecnologiche. Dato il core business caratteristico e la posizione di mercato occupata, anche in questo caso la prevenzione sarà preponderante in quanto i rischi sono percepiti come stabili, misurabili e persistenti e l'infrastruttura tecnologica fa da supporto alle operazioni principali. Anche in questo caso i responsabili delle infrastrutture IT ricoprono un ruolo marginale nella gestione della società e nel raggiungimento del suo scopo sociale. Questo però non sta a significare che non debba essere posta attenzione sulla gestione e sulla sicurezza della tecnologia, in quanto, come abbiamo avuto modo di discutere in precedenza, anche società teoricamente distanti dal mondo dell'IT in se per se, ci si stanno avvicinando mano mano sempre più, dapprima sfruttando i nuovi strumenti di supporto alle normali operazioni quotidiane (dalla tenuta della contabilità alla scansione dei prodotti venduti) e, più recentemente per modernizzare l'immagine della società; ad esempio essendo attivi sui social media. Questo ultimo aspetto si sta rilevando sempre più un fattore di successo in quanto, in questo modo i clienti hanno la possibilità di interagire direttamente con la società, potendo ad esempio esprimere giudizi personali. Altro uso che se ne fa delle nuove tecnologie, sono ad esempio la raccolta dei dati dei clienti, la loro archiviazione e la loro analisi attraverso procedure di data mining al fine di

ottenere informazioni sulle loro preferenze, sull'ammontare della loro spesa, sulle tipologie di prodotti acquistati e via dicendo.

Potrebbero farsi considerazioni analoghe a quelle già fatte per i casi precedenti anche per quanto riguarda la strutturazione della società secondo il TFI model. Sul lato tecnico, si è in presenza di una struttura sostanzialmente identica alle altre, dove la strumentazione tecnologica principale consiste nei computer, nei database, nelle casse, nei POS, nelle strumentazioni necessarie alla gestione del magazzino (come potrebbero esserlo ad esempio i lettori RFID) e dove il network interno non è particolarmente sviluppato se paragonato a quello di altre società come quelle informatiche o quelle bancarie. Per quanto riguarda invece, gli aspetti formali ed informali, vi è una generale messa in regola con gli standard minimi e un non troppo sviluppato sistema di politiche di sicurezza interno. Anche in questa realtà, la protezione della riservatezza, integrità e disponibilità dei dati diventa di fondamentale importanza, dal momento che per le ragioni già largamente esposte nei casi precedenti, non solo si ha la necessità di proteggere informazioni fondamentali all'operatività aziendale ma anche di proteggere tutti quei dati relativi ai clienti che, come sopra discusso, risultano fondamentali per mantenere l'ordine pubblico.

Come spesso accade, non importa quanto una società possa investire in sicurezza informatica, se qualcuno vuole ottenere un accesso non autorizzato ai sistemi informatici, sicuramente lo farà. Questo rispecchia quanto successo a Home Depot, la quale nonostante investisse una notevole parte delle proprie risorse disponibili in sicurezza dell'IT (tenendo sempre in considerazione che, la maggior parte delle aziende operanti nel medesimo mercato ne investano un piccola parte) e, nonostante avesse pianificato di li a poco l'aggiornamento delle misure di sicurezza sulle proprie infrastrutture, nella seconda metà del 2014, la società venne colpita da un attacco informatico. Nel settembre 2014, Home Depot afferma di aver subito un attacco informatico, il quale le ha sottratto un'enorme quantità di dati estremamente riservati. Gli hacker sono riusciti a sviluppato un malware ad hoc, creato appositamente per questo attacco, capace di raccogliere i dati sensibili in transito nei POS (quali ad esempio i nominativi dei clienti e le informazioni delle carte di credito come numero di carta e pin). Il malware utilizzato, essendo stato sviluppato esclusivamente per questo attacco, non era mai stato notato prima d'ora ed era in grado di superare le misure di sicurezza adottate, tra cui gli antivirus installati sui computer. Dapprima si era pensato che gli hacker fossero riusciti ad ottenere l'accesso ad informazioni riservate come password e dati di carte di credito/debito mentre, successivamente si è venuto a scoprire che questi non siano stati capaci di arrivare a

tali informazioni. Tuttavia, sono riusciti ad ottenere l'accesso ai file dove vi erano registrati tutti gli indirizzi email della clientela. Dopo aver appreso l'entità del danno e, aver stimato il costo dell'attacco (che, nel peggiore dei casi toccherebbe la cifra di 3 miliardi di dollari) la società si è curata di pubblicare sul proprio blog, un documento dove denunciava l'accaduto ed informava i propri clienti che vi era la possibilità che le loro email fossero state rubate e quindi di porre attenzione qualora si ricevessero email sospette da indirizzi sconosciuti. Oltre ciò, la dirigenza ha imposto la conclusione del programma di aggiornamento di sicurezza dell'infrastruttura informatica entro il mese di settembre, per gli store su suolo USA e, anticipandolo ai primi mesi del 2015, per gli store canadesi.

Secondo lo schema del TFI model invece, possiamo affermare come a nostro avviso nell'incidente rilevi soprattutto l'aspetto formale. In questo caso possiamo evidenziare come si sarebbe potuta evitare l'intrusione tramite l'adozione di metodologie atte a contrastare l'istallazione e l'esecuzione di programmi sconosciuti. Come nel caso precedente, una di queste metodologie sarebbe quella delle whitelist. In questo caso, solo una lista di programmi ben definiti e conosciuti, possono essere istallati sulle macchine e possono quindi essere eseguiti. In questo modo, programmi sconosciuti (come il malware utilizzato) non avrebbero ottenuto i permessi necessari e non avrebbero potuto compiere il proprio dovere. Per quanto riguarda l'aspetto tecnico ed informale, non sembra si possa imputare alcuna mancanza.

In definitiva, come per gli altri due casi sopra esposti, viene confermato il fatto che, società operanti in settori di mercato caratterizzati da un basso turnover delle strumentazioni tecnologiche, come potrebbe essere appunto quello dei grandi distributori di beni di consumo quali sono TJX, Target e Home Depot, i rischi vengono percepiti come stabili e prevedibili. Questo porta alla conclusione che questo particolare tipo di società reagisca in maniera più lenta e graduale a situazioni dove viene messa in pericolo la propria sicurezza. Questa caratteristica fa si che però venga posta molta attenzione alla prevenzione, portando ad esempio alla stesura di severe politiche di sicurezza interne (non necessariamente di natura informatica, infatti potrebbero ad esempio esservi regole che garantiscano la corretta conservazione dei prodotti o che evitino il furto di questi da parte dei dipendenti) o l'instaurazione di severi controlli all'accesso alle strumentazioni informatiche.

Dopo aver analizzato delle società dove il paradigma di prevenzione la fa da padrona, andremo ora ad analizzare tre casi che hanno coinvolto società di natura e caratteristiche differenti. Queste operano nel settore bancario, dei servizi di pagamento e nella vendita di beni di consumo tramite internet (e-commerce) pertanto, sono caratterizzate da un differente

approccio agli incidenti. Data la loro natura, l'organizzazione e la posizione di mercato occupata, vedremo come queste siano caratterizzate da un bilanciamento più "equo" tra prevenzione e risposta, dove si cerca di mantenere un equilibrio tra i due paradigmi. Questo perché operano in un ambiente complesso e a rapida evoluzione, dove le pressioni dei competitors portano al continuo bisogno di aggiornare il modello di business adottando soluzioni IT sempre più innovative. Come risultato, queste società vanno continuamente incontro a nuovi rischi e la gestione della sicurezza informatica si focalizza sulla protezione di una vasta gamma di risorse.

3.5 Caso quattro: J.P. Morgan Chase & Co

J.P. Morgan Chase & Co. è una società finanziaria con sede a New York, ed è leader nei servizi finanziari globali. Attualmente serve più di 90 milioni di clienti.
Come accennato poco sopra, JP Morgan e le altre organizzazioni attive nel medesimo settore, operano in un contesto caratterizzato da un'alta evoluzione sia tecnica che tecnologica e dove vi è quindi la necessità di adottare continuamente nuove soluzioni. Come risultato si ha un ambiente pieno di nuove tipologie di rischi, i quali impongono al management un rapido adattamento delle infrastrutture qualora venissero ad esistenza nuovi pericoli. In un contesto simile, l'organizzazione sa che non è possibile stabilire a priori quanto questi siano prevedibili, persistenti e misurabili. Per tale ragione una valutazione dei rischi e un'analisi dell'impatto – sia in termini economici che strutturali - di un incidente può essere utile ad ottenere un'istantanea delle vulnerabilità proprie dell'organizzazione. In una società come JP Morgan, il ruolo dell' IT è sicuramente di fondamentale importanza. L'attività bancaria necessita del supporto informatico anche per le operazioni più semplici e, sarebbe ormai impensabile esercitare tale attività senza l'uso della tecnologia. Questa necessità, è confermata dal fatto che, ad esempio JP Morgan investa una cifra come 250 milioni di dollari annui in sicurezza informatica. In un contesto simile, la figura del CISO è sicuramente di fondamentale importanza, in quanto ha il compito di gestire un vastissimo network nel quale transitano dati altamente sensibili e, una loro possibile perdita causerebbe dei danni incalcolabili. In questo ambiente quindi la sicurezza dell'IT è fondamentale e, proprio per queste ragioni viene messa a budget una somma tanto ingente. Il bilanciamento tra

prevenzione e risposta quindi, sarà sicuramente più equilibrato rispetto ai casi visti in precedenza. In un contesto simile, la società opera in ambienti con differenti tipologie di rischi, alcuni stabili, altri instabili dove la gestione delle informazioni richiede una posizione di bilanciamento tra prevenzione e risposta.

Riferendoci ora alla protezione della riservatezza, disponibilità ed integrità dei dati, questa risulta essere molto più necessaria, in termini di possibili danni che verrebbero ad esistenza nel caso di incidente, rispetto alle realtà precedenti. In questo caso, la perdita della disponibilità o integrità dei dati causerebbe numerosi problemi di grandi dimensioni. Questo perché, basandosi fortemente sulla tecnologia, la perdita di queste proprietà, renderebbe inutilizzabili i dati in possesso e quindi sostanzialmente renderebbe vane le operazioni proprie dell'attività bancaria. Si pensi ad esempio al caso in cui non sia possibile ottenere informazioni riguardo le disponibilità liquide di un cliente. Questo non avrebbe accesso al proprio conto corrente e, di conseguenza non potrebbe utilizzare gli usuali servizi bancari (come il prelievo dagli sportelli ATM o il pagamento tramite carta di credito). Non meno rilevante è il tema della riservatezza. Chiaramente, nel malaugurato caso si perdesse tale caratteristica dei dati (ciò che è accaduto in questo caso), le conseguenze sarebbero catastrofiche. I clienti potrebbero vedersi privati dei propri risparmi e, tutte le informazioni sensibili come dati personali, situazioni economiche, dati su prestiti e altre informazioni varie, potrebbero essere usate per ulteriori azioni criminose.

Concentrando la nostra attenzione sull'accaduto, possiamo dire che tutto cominciò nel giugno 2014 quando il computer di un dipendente della banca fu infettato da un malware, il quale fu capace di rubare delle credenziali d'accesso riservate. Una volta collegatosi alla rete tramite le credenziali sottratte all'ignaro dipendente, l'hacker fu in grado di sfruttare il login appena rubato come punto di partenza per poi ottenere i permessi necessari per poter accedere al network aziendale. Da questo punto, è stato possibile, tramite un altro virus progettato proprio per l'occasione, penetrare ai più alti livelli di sicurezza e riuscire così ad ottenere il controllo di oltre 90 server della banca. Per evitare di essere scoperto, l'hacker ha svolto il proprio lavoro molto lentamente, sottraendo le informazioni poco alla volta nell'arco di molti mesi. L'intrusione non sarebbe stata scoperta se, nell'agosto dello stesso anno, non fosse stato violato anche uno sito internet partner della banca. Avviate le indagini su quest'ultimo caso, si è venuto così a scoprire che anche JP Morgan aveva subito un attacco direttamente alle proprie strutture, compromettendo milioni di dati dei clienti. Il numero di dati sottratti è altissimo. 83 milioni di dati riferiti ad altrettanti soggetti. Fortunatamente però gli hacker sono

stati in grado di entrare in possesso "solamente" dei nominativi, indirizzi di residenza, numeri telefonici, indirizzi email, senza che vi sia stata la possibilità di accedere ad informazioni più strettamente confidenziali come quelle economico-finanziarie. Nonostante gli ingenti investimenti in sicurezza, anche un colosso come JP Morgan è stato colpito da un attacco di questo genere. Come è naturale pensare, è impossibile programmare un sistema informatico in grado di essere sicuro al 100% e, questo episodio ha confermato tale assunto (per essere completamente esenti da ogni rischio, come affermato in teoria, si dovrebbe distruggere la tecnologia, ad esempio smembrando il sistema informatico. Chiaramente in una realtà di questo genere non sembra essere una strada percorribile). Una volta che l'attacco fu individuato, fu dato il via alle indagini. L'accaduto è stato denunciato alle autorità competenti e la banca si è servita di alcuni dei più grandi nomi operanti nel settore della sicurezza informatica per far si che un simile evento non possa ripetersi in futuro. Le indagini hanno chiarito che vi era più di un punto debole nelle misure preventive adottate ed infatti si possono scovare problematiche sia sul fronte tecnico, sia su quello formale che su quello informale.

Per quanto riguarda il primo, al momento della configurazione del network, i progettisti hanno fornito un eccessivo numero di permessi anche a coloro i quali non erano necessari. Per spiegarsi meglio, il dipendente in questione, da dove cui il tutto si è scaturito, possedeva permessi di accesso a zone della rete di non sua competenza. Si sarebbe dovuto suddividere il network in dei compartimenti stagni, dove nel caso in cui si verificasse un accesso non autorizzato, l'intruso non avrebbe avuto la possibilità di accedere alla gran parte dei dati archiviati. Al momento della progettazione, si sarebbe dovuto restringere il numero dei permessi in possesso ad ogni singolo dipendente, in modo tale che non sarebbe stato possibile accedere a particolari sezioni critiche. Ad esempio, l'impiegato allo sportello non dovrebbe avere i permessi necessari ad accedere alla piattaforma di controllo dei terminali. Gli ingegneri che si occupano della gestione dell'infrastruttura hardware, non dovrebbero aver accesso alle informazioni strategiche del management. In JP Morgan però, il dipendente in questione aveva più permessi di quanti effettivamente ne avrebbe avuto bisogno (dalle indagini risulta che aveva accesso a circa il 14% in più dei dati di sua competenza). Esistono varie metodologie che avrebbero sopperito a questa mancanza. Uno di questi è il Network Access Control (NAC), il quale è capace di rilasciare l'accesso al richiedente solo dopo aver scansionato il computer alla ricerca di un possibile malware in modo da essere certo che la richiesta d'accesso sia effettuata da un avente diritto. Si sarebbero potute adottare ulteriori

misure di sicurezza anche sul lato formale e, infatti nonostante la banca fosse in linea con i vari standard di sicurezza generalmente imposti e, nonostante spendesse un'ingente somma in cyber security, i responsabili della stesura delle politiche di sicurezza interne non hanno pensato di adottare meccanismi di login più sicuri come ad esempio il metodo dell'autenticazione a due fattori, il quale richiede una one-time password (OTP) prima di fornire i permessi per l'accesso ad informazioni riservate. Sul piano informale invece, sono state riscontrate lacune per quanto riguarda il comportamento del dipendente. Non si hanno notizie ufficiali su come gli hacker siano riusciti a compromettere il pc iniziale ma, molto probabilmente, questo è accaduto tramite l'uso di email infette. Esistono numerosi modi per evitare questo genere di attacco ed uno di questi è, ovviamente tenere aggiornato l'antivirus e/o installare un Host-Based Intrusion Prevent System (HIPS) il quale fornisce maggiore protezione rispetto ad un antivirus tradizionale. In definitiva, sembra che il sistema informatico di JP Morgan non sia sufficientemente protetto per garantire la sicurezza dei propri dati. Ovviamente ciò non sarebbe ammissibile, ne tantomeno giustificabile sotto il punto di vista della spesa e del numero di operatori impegnati costantemente a garantire la massima sicurezza dei dati archiviati. Questo caso mostra come tale settore di mercato debba costantemente fronteggiare nuovi rischi derivanti dalla sua mutevolezza e dalla sua variabilità. Come abbiamo affermato in precedenza, in un contesto di questo genere, l'organizzazione sa che non è possibile stabilire a priori quanto i rischi siano prevedibili, persistenti e misurabili; pertanto vengono adoperate misure di analisi in modo da valutare i rischi che vengono corsi. Oltre a misure tecniche, è importante anche che vengano adottate particolari politiche di sicurezza atte ad evitare la perdita della riservatezza, integrità e disponibilità dei dati, come potrebbero esserlo i disaster recovery plan. Possiamo speculare che la banca, data l'enorme spesa in sicurezza e la consapevolezza della tipologia di mercato in cui opera, abbia adottato numerose e generose politiche di questo tipo. In fine, come affermato anche nella teoria, è di fondamentale importanza riuscire a controllare e gestire il lato comportamentale delle figure umane all'interno dell'organizzazione. Queste sono le più imprevedibili e quelle che potrebbero causare i danni maggiori. Utili metodologie per diminuire il rischio di questo genere sono ad esempio la tenuta di corsi specializzati per i dipendenti sulle normali pratiche di sicurezza informatica, e sui pericoli e gli effetti dell'ingegneria sociale.

3.6 Caso cinque: Heartland Payment Systems Inc.

Heartland Payment Systems (HPS) è una società che si occupa di pagamenti elettronici. Fondata nel 1997 da Robert O. Carr, con sede in Princeton, New Jersey, è una delle più grandi società nel suo settore.

Come JP Morgan, anche HPS, opera in un contesto di mercato particolare, caratterizzato da una continua evoluzione tecnologica, dove viene richiesto un costante aggiornamento delle strumentazioni al fine di riuscire a fornire sempre i migliori servizi nel minor tempo possibile e nei modi più sicuri. Di pari passo però avanzano anche i possibili rischi che tali imprese affrontano. Come avremo modo di vedere più nel dettaglio nel corso di questo capitolo e, come già è stato esposto nel capitolo precedente, tali rischi crescono con l'aumentare della tecnologia adottata, delle componenti e delle loro connessioni. In una realtà come quella delle società finanziarie, la tecnologia utilizzata è spesso molto complessa, pertanto occorre effettuare profonde analisi dei rischi che vengono corsi qualora venga adottata una particolare tecnologia e vengano maneggiati determinati tipologie di dati. Possiamo affermare infatti che, il rischio di subire un attacco informatico aumenta con l'aumentare dei dati posseduti, con l'aumentare della sensibilità di questi dati e con l'aumentare della tecnologia utilizzata. Con il termine incidente però non si intende solamente la possibilità di essere bersagli di attività criminose, bensì può identificarsi anche con eventi accidentali e del tutto scollegati da quest'ultimo come ad esempio, lo scoppio di un incendio, l'allagamento degli spazi adibiti ai server o qualunque altra forma di incidente che non sia un attacco informatico. Chiaramente la possibilità che si verifichi un tale evento non è data ne dalla sensibilità dei dati ne tantomeno dal numero di questi ma, solamente dalla tecnologia adottata e dal comportamento umano di coloro che maneggiano tali strumentazioni.

Tornando al caso in questione, per quanto riguarda la protezione della disponibilità, riservatezza ed integrità dei dati anche nella realtà di HPS vale quanto detto per JP Morgan. Si ha la necessità di proteggere i dati da qualsiasi tipo di danneggiamento in modo da garantire sempre il corretto funzionamento. La perdita di riservatezza, anche in questo caso arrecherebbe gravi danni ai clienti in quanto, maneggiando informazioni sensibili come le credenziali d'accesso ai conti correnti o i nominativi dei propri clienti, verrebbe violata la privacy e verrebbe corso il rischio di subire un furto sul proprio conto corrente. Anche in questo caso però, l'incidente avvenuto alla società riguarda la perdita di riservatezza dei dati.

Nel 2007, un gruppo di hacker è riuscito a fare breccia nel network di HPS, riuscendo ad ottenere l'accesso a dati come quelli riferibili a carte di credito, nominativi dei clienti e tutti i dati mossi attraverso il sistema.

Per infiltrarsi e riuscire così nell'intento, gli hacker si sono serviti di una tecnica chiamata SQL injection[9]. Questa è una tecnica propria dell'hacking, che mira a colpire le applicazioni web che si appoggiano su un DBMS di tipo SQL. Questo exploit sfrutta l'inefficienza dei controlli sui dati ricevuti in input ed inserisce un codice maligno all'interno di una query SQL. Le conseguenze prodotte sono imprevedibili per il programmatore: l'SQL injection permette al malintenzionato di autenticarsi con ampi privilegi in aree protette del sito anche senza essere in possesso delle credenziali d'accesso e di visualizzare e/o alterare dati sensibili. Queste inefficienze non erano mai state identificate prima, ne tramite i controlli periodici che vengono effettuati annualmente sulla struttura, ne tramite il sistema di controlli interno ad azione continua. Nonostante esistesse da diversi anni, la falla non era mai stata ne identificata, ne sfruttata prima d'ora. Una volta che gli aggressori sono riusciti ad invadere il sistema, è stato istallato un programma di sniffing[10], capace di raccogliere le informazioni in transito sulle apparecchiature della società. I dati rubati si riferiscono a dati relativi a carte di credito, nominativi dei clienti e tutti i dati mossi attraverso il sistema. In un sistema tanto complesso quanto quello di HPS, risulta impossibile riuscire a realizzare una struttura informatica priva di rischi e infatti, nonostante fosse in linea con i vari standard di sicurezza, nonostante avesse programmato un continuo controllo delle proprie strumentazioni e dei propri sistemi, sfruttando una falla nella scritturazione del codice, gli hacker sono comunque riusciti ad invadere il sistema. A seguito del furto di quasi 130.000.000 di dati, i costi furono altissimi. Si stima che questi raggiungessero i 170 milioni di dollari.

Prima dell'accaduto, Heartland non era dotata di un vero e proprio incident recovery plan e questo lo espose ad ulteriori perdite. Grazie all'accaduto però, attivando il paradigma di risposta, la società si è prima di tutto dotata di un documento di questo genere, in modo tale da evitare di commettere lo stesso errore due volte e, dopo di che si è mossa in prima linea per contrastare attacchi come quello appena subito, concentrandosi anche nella stesura di standard ulteriormente sicuri, in modo tale da ridurre il rischio del verificarsi nuovamente di un evento simile. Anzitutto, HPS diventò molto più aggressiva in termini di sicurezza, concentrandosi nella realizzazione di politiche ad hoc atte a garantire la massima sicurezza ogni qualvolta

[9] SQL injection http://it.wikipedia.org/wiki/SQL_injection

[10] Sniffing http://it.wikipedia.org/wiki/Sniffing

avvenga un pagamento, sfruttando un nuovo sistema end-to-end. La criptazione dei dati avviene in ogni step delle operazioni per completare una transazione; dalla prima "strisciata" sul POS alla ricezione del pagamento. Inoltre, HPS si è impegnata, assieme ad una società Taiwanese, nella realizzazione di una particolare tipologia di POS, estremamente sicuro e dotato di un sistema di criptazione inserito direttamente nell'hardware. E' stato inoltre istituito il gruppo FS-ISAC volto a promuovere lo scambio di informazioni tra più aziende in materia di cyber security. Possiamo quindi affermare che l'incidente abbia attivato nel migliore dei modi il meccanismo di risposta proprio di una società come Heartland, la quale opera in un contesto di mercato tanto variabile quanto imprevedibile.

Tornando all'incidente, possiamo rilevare carenze solamente nella parte formale identificabile dal TFI model. Nonostante HPS fosse in regola con gli standard di sicurezza PCI DSS, gli intrusi sono riusciti ugualmente ad infiltrarsi nel sistema. Questo sta a significare che tali standard rappresentano solamente le difese minime che una società di questo genere dovrebbe possedere e, può evidenziarsi come ci sia la necessità di ulteriori aggiornamenti per poter affermare che tali standard siano realmente efficaci. Ciò che è stato eclatante in questo caso, è il fatto che la società non possedeva alcun tipo di piano nel caso in cui si fosse verificato un incidente. Come ripetuto in più occasioni, l'adozione di politiche di sicurezza interne è un fattore chiave per scongiurare la perdita definitiva di dati utili al proseguimento dell'attività. In numerosi casi, la mancata adozione di tali politiche ha fatto si che, dopo il verificarsi di un incidente (non necessariamente di natura informatica), la società abbia dovuto dichiararsi fallita in quanto è stato perso un elevato numero di dati e informazioni utili alla continuazione aziendale.

Anche questo caso risulta emblematico per il nostro studio, in quanto viene evidenziato il fatto che, come nel caso precedente, non importa quanto venga speso e quanto venga curata l'infrastruttura tecnologica, una parte di questa sarà perennemente esposta ad un certo livello di rischio e, che tale livello cresca all'aumentare della complessità tecnologica, della tipologia di dati posseduti e della quantità di questi. Viene inoltre sottolineata l'importanza della stesura di piani e politiche interne atte a riprendere, nel migliore dei modi il proseguo dell'attività qualora si verificasse un incidente.

3.7 Caso sei: eBay Inc.

eBay Inc. è un sito di aste on-line fondato il 6 settembre 1995 da Pierre Omidyar; in Italia è arrivato nel 2001 rilevando il sito iBazar. eBay è una piattaforma web (marketplace), di fatto molto simile ad un sito di e-commerce, che offre ai propri utenti la possibilità di vendere e comprare oggetti sia nuovi che usati, in qualsiasi momento, da qualunque postazione Internet e con diverse modalità, incluse le vendite a prezzo fisso e a prezzo dinamico, comunemente definite come "aste online".

Diversamente dalle ultime due società appena analizzate (JP Morgan e HPS), eBay non si occupa di servizi finanziari (nonostante dal 2002 al 30 settembre 2014 la società PayPal fosse controllata dal colosso delle aste online). eBay è una società basata interamente sull'informatica e sul mondo di internet, impiantando appunto il suo core business su tale tecnologia. In questa realtà il ruolo del CISO è sicuramente di grande rilevanza, in quanto ogni decisione relativa all'adozione di un nuovo progetto dovrà passare sotto il suo consenso. Questo però non sta a significare che tale ruolo, in un contesto societario come quello di eBay, debba necessariamente essere più influente di quello di JP Morgan o HPS. Queste tre società, nonostante il differente modo di operare e il differente segmento di mercato conteso, a mio avviso adottano il medesimo grado di mix tra prevenzione e risposta. Questo perché anche il grado di complessità tecnologica e il contesto ambientale sono molto simili. Da un lato abbiamo due colossi dei servizi finanziari che, come descritto in precedenza, hanno una struttura informatica molto elaborata e ogni anno vengono spesi centinaia di milioni di dollari nella sola sicurezza informatica. Dall'altro lato vi è un altro colosso, questa volta operante nel settore della vendita online e con una struttura informatica similmente complessa. Tutte e tre le società inoltre operano in un mercato dove la tecnologia la fa da padrona e, proprio per questo motivo rende il contesto operativo, l'ambiente e i rischi estremamente variabili e mutevoli. Infatti, come è sufficiente una minima – purché brillante – innovazione nel campo informatico per stravolgere il settore, è altrettanto "semplice" riuscire a sfruttare eventuali debolezze in un sistema informatico tanto complesso al fine di entrare in possesso di dati riservati. Inoltre, tali realtà sono tutte in possesso di informazioni riservate. JP Morgan detiene informazioni personali, posizioni economico-finanziarie e l'accesso ai conti correnti dei propri clienti. HPS, nel ruolo di gestore dei pagamenti elettronici possiede le informazioni

necessarie per effettuare acquisti tramite l'elaborazione dei dati delle carte di credito. Anche eBay elabora e archivia i dati strettamente personali dei propri clienti (come ad esempio indirizzo di residenza, recapito telefonico, nominativi e così via) e inoltre è in possesso dei loro dati finanziari per poter effettuare acquisti online. Tutte e tre le società quindi, posseggono informazioni che potrebbero far gola a degli hacker. Per queste ragioni (grado di complessità tecnologica, posizione di mercato occupata e rilevanza delle informazioni possedute) ritengo che tali organizzazioni adottino il medesimo grado di mix di prevenzione e risposta qualora debbano fronteggiare un incidente. Anche l'aspetto formale e informale a mio avviso sono molto simili. Questo perché, tutte e tre le società devono rispondere dell'adozione degli standard di sicurezza quali i PCI DSS e devono garantire il medesimo grado di protezione delle informazioni, istruendo e proteggendo anche il personale dall'evenienza di un incidente. Sul piano tecnico invece, a mio avviso possono sussistervi delle differenze soprattutto tra le prime ed eBay. Questo perché il servizio offerto dai due gruppi (JP Morgan e HPS vs eBay) è differente. Da un lato abbiamo la necessità di creare un network in grado di collegare centinaia di migliaia di computer dislocati per tutto il globo, riuscendo, però al contempo, a controllarli anche da remoto. Si ha la necessità (soprattutto nel caso di JP Morgan) di creare un sistema che riesca a connettere l'intero ecosistema della banca ai vari network infra-bancari riuscendo però, allo stesso modo, a garantire un'agile prestazione di tutti i servizi offerti. Dall'altro lato invece, abbiamo una società costituita da poche decine di migliaia di computer e poche sedi operanti in diversi paesi. Il network richiesto in quest'ultimo caso, avrà sicuramente un numero inferiori di nodi (e quindi di connessioni) ma questo non sta a significare che non abbia bisogno di una potenza di calcolo ed un'efficienza pari a quella delle altre due società.

Prendendo ora in considerazione il caso proposto, possiamo evidenziare come nei mesi di febbraio-marzo 2014, la società sia stata vittima di un incidente informatico. L'attacco è stato reso possibile grazie alla destrezza degli hacker nel manipolare tecniche di ingegneria sociale. Questi ultimi, sono riusciti ad entrare in possesso di alcune credenziali d'accesso di un ristretto numero di dipendenti. Probabilmente queste informazioni sono state ottenute grazie ad un attacco di spear phishing[11]. Una volta ottenuti i permessi d'accesso, gli hacker sono riusciti ad entrare all'interno del network ed avere accesso alle informazioni contenute nei database. Fortunatamente gli intrusi non sono riusciti ad arrivare ai dati delle carte di credito in quanto questi erano memorizzati su database differenti (quelli di PayPal). Quello di eBay,

[11] Cos'è lo spear phishing? http://www.kaspersky.com/it/internet-security-center/definitions/spear-phishing

si è rivelato uno dei più grandi data breaches della storia, in quanto sono stati sottratti circa 145 000 000 di dati utente e, dimostra ancora una volta come anche le compagnie dotate dei migliori sistemi di sicurezza possano essere soggette a simili incidenti.

Analizzando il grado di prevenzione adottato, possiamo affermare che il sistema di sicurezza interno era affidabile tanto che la causa dell'attacco non è attribuibile ad un errore presente nel sistema di sicurezza bensì in un errore umano. L'efficacia del sistema di sicurezza eBay è stato confermato dal fatto che oltre ad essere in linea con gli ormai soliti standard di sicurezza, gli hacker non sono riusciti ad ottenere alcuna informazione riguardo i dati finanziaria dei clienti, dal momento questi erano memorizzate su un network separato. Chiaramente ciò non sta a significare che l'accaduto non possa mettere in pericolo l'identità dei clienti che hanno subito il furto. Sono stati infatti sottratti dati come nominativi dei clienti, indirizzi email, indirizzi di residenza, numeri telefonici, password criptate e date di nascita.

La risposta a tale evento, non è stata però altrettanto virtuosa quanto l'adozione delle profonde misure di sicurezza di prevenzione esposte poc'anzi. Questo perché i clienti non furono informati dell'accaduto se non solo due settimane dopo l'incidente. Nulla fu scritto sul blog ufficiale della compagnia. Due settimane dopo, ai clienti venne esposto il fatto tramite un'email, la quale conteneva chiarimenti riguardo l'intrusione, cosa sia stato compromesso e delle best practice per mantenere protetti i propri dati personali. eBay inoltre, denunciando l'accaduto alle autorità competente, è entrata in collaborazione con l'FBI e con compagnie private per far luce sull'accaduto.

Nulla può annoverarsi per quanto riguarda l'aspetto tecnico e formale in quanto, come già ampiamente esposto in precedenza, la società aveva adottato tutte le misure di sicurezza (sia interne che esterne, sia tecniche che non) necessarie a ridurre al minimo il rischio di incidenti. Possiamo però individuare la causa dell'attacco sul fronte del comportamento umano e quindi, sul lato informale del nostro TFI model. Come si evidenzia nella teoria dell'ICT, l'errore umano è la principale causa di eventi sconvenienti e talvolta catastrofici per un sistema informatico e in particolar modo per un'intera azienda. Questo perché, mentre un sistema informatico, teoricamente possa essere perfetto al 100%, il comportamento umano, invece, funziona in maniera differente. Ognuno agisce secondo scopi e metodi diversi e questa è la causa principale della rischiosità del comportamento umano. A confermare tale assunto, il caso di eBay è emblematico, dove è stato per l'appunto un comportamento umano errato (l'essere stati adescati da email fraudolente) a causare l'intrusione. Tale rischiosità dei

comportamentale, potrebbe essere mitigata tramite la tenuta di corsi formativi per i dipendenti e un maggior grado di sicurezza qualora questi possano accidentalmente compiere errori.

3.8 Caso sette: Adobe Systems Inc.

La Adobe Systems Inc. è una software house statunitense con sede a San Jose in California, nota soprattutto per i suoi prodotti di video e grafica digitale. E' inoltre, una delle società più famose e ricche del pianeta.

Nonostante l'assetto organizzativo sia quello della classica public company statunitense, un po' come quelle viste fino ad ora; dato il suo segmento di mercato estremamente tecnico ed incentrato sullo sviluppo del software e, data la sua struttura organizzativa, possiamo affermare come sotto il punto di vista funzionale sia molto diversa dalle altre società operanti in mercati più "tradizionali". Differentemente da TJX o Target, Adobe non necessita di numerose sedi sparse per il globo, anzi la maggior parte delle decisioni, dei progetti e degli sviluppi nascono, si sviluppano e vengono distribuiti proprio dalla sede centrale (come succede un po' per tutte le software house). Dato questo assetto però, non bisogna cadere nell'errore che, data la sua scarsa presenza sul territorio, non necessiti di un network, o di un sistema informatico ben strutturato. Proprio per la sua natura informatica invece, può notarsi come l'intera organizzazione poggi interamente le proprie fondamenta sul reticolo di componenti che costituiscono il network aziendale e l'intera struttura IT. Chiaramente, essendo leader nel settore e, utilizzando la tecnologia come proprio strumento di successo, il board di dirigenti responsabili della sicurezza sia fisica che software, avrà sicuramente una forte autorità nel prendere le decisioni all'interno del CDA in quanto questi sono responsabili della sicurezza e, dovendo reagire sia a nuovi che vecchi pericoli giocando un ruolo chiave per l'organizzazione.

Date quindi tali caratteristiche strutturali, data la presenza in un mercato e un contesto estremamente mutevole, possiamo affermare come Adobe sicuramente concentri il massimo delle proprie risorse nel paradigma di risposta. Questo perché, in un contesto come quello in cui opera Adobe, i rischi vengono visti come imprevedibili e non misurabili. Ogni nuova componente viene vista come una potenziale fonte di debolezze. Si pensi al caso in cui vi sia un adattamento o un aggiornamento di una componente software sviluppata da Adobe. Se precedentemente al cambiamento, il sistema era conosciuto in ogni suo minimo dettaglio e si

erano riusciti a scovare e colmare tutte le sue debolezze, una volta avvenuto l'aggiornamento possono riscontrarsi nuove problematiche. Si devono nuovamente passare in rassegna tutte le minime debolezze che questo potrebbe avere e, nonostante ciò, non si sarebbe ancora certi che tale nuova componente sia totalmente sicura. In quanto software house, il compito di verificare la sicurezza di tali adattamenti spetta ad Adobe e, nel malaugurato caso che problematiche relative allo sviluppo del software si presentassero successivamente alla vendita del prodotto, la società sarebbe chiamata in causa per risarcire i danni (potenzialmente enormi) derivanti da tale malfunzionamento. Questo spiega perché una società con queste caratteristiche dovrebbe sbilanciarsi più sulla risposta che sulla prevenzione qualora debba affrontare il rischio di incidenti. La sicurezza chiaramente deve essere garantita anche alle proprie infrastrutture e, anche in questo caso vale quanto detto sopra; ogni minimo cambiamento potrebbe essere portatore di possibili danni futuri.

Sicuramente in una società del genere si deve porre molta attenzione all'aspetto tecnico di tutta l'organizzazione. Questo soprattutto nella sicurezza fisica delle apparecchiature (come database, server ecc.) e nella sicurezza dei computer, in quanto la loro disponibilità deve essere sempre garantita e in funzione. Sarebbe impensabile non adottare politiche di sicurezza stringenti anche per quanto riguarda la riservatezza dei dati, sia per garantire la sicurezza delle informazioni attinenti ai progetti, ai servizi aziendali, sia per quanto riguarda la protezione di quei dati sensibili propri dei clienti come potrebbero esserlo le credenziali d'accesso (pin e password) e dati finanziari sensibili (come i dati d'accesso alle carte di credito).

Proprio su questo fronte, nell'ottobre 2013, la società ha subito un attacco diretto ai propri database dove erano archiviate le informazioni sensibili dei propri clienti. Un gruppo di hacker è riuscito a penetrare all'interno del sistema di Adobe e ad ottenere milioni di dati criptati, incluse password e altre credenziali (come il pin dei conti). Dopo il furto, i dati comparvero online su un forum di una delle più grandi comunità di hacker dove vennero resi pubblici attraverso due file. I dati erano stati postati sia nella versione criptata che non, dando così modo agli altri utenti di poter usufruire di tali informazioni. L'accaduto evidenzia come il sistema di criptazione adottato (prevenzione) non fosse adeguato alla sensibilità dei dati archiviati e al contesto di operatività della società. La metodologia di criptazione adottata per proteggere tali dati, si è rilevata insufficiente causando così gravi danni ai clienti, i quali corrono/hanno corso il rischio di subire ulteriori furti sui propri conti bancari e accessi non autorizzati in altri siti dove venivano utilizzate le medesime credenziali d'accesso. Volendo fornire un'analisi più dettagliata su quale sia il motivo per la quale non è stata sufficiente la

metodologia di protezione dei dati, possiamo affermare che durante la fase di criptazione non sono state adottate le migliori tecniche crittografiche, in quanto i dati non erano criptati secondo la procedura hash+salt[12]. Questa garantisce una maggiore protezione a seguito di un eventuale furto di dati. Secondo quanto emerso dalle indagini, Adobe infatti per la messa in sicurezza dalla informazioni da lei possedute, utilizzava la sola procedura di hash (senza applicarne il sale). Questo era oltremodo sconsigliato dagli standard di sicurezza generali, il quale suggeriva l'adozione di metodologie più sicure. Avvenuta l'intrusione però la società non si è fatta cogliere impreparata. La dirigenza ha imposto l'immediata adozione dei criteri di sicurezza più sicuri e l'immediato reset delle password, al fine di rendere impossibile l'accesso agli account tramite le credenziali rubate. La società ha inoltre inviato delle email di notifica ai propri clienti, dove venivano avvisati dell'accaduto, dove erano contenute delle istruzioni per creare una nuova password e dove erano indicate delle best practice al fine di evitare che coloro che siano entrati in possesso di quei dati, possano sfruttarli anche su altri network. Sono stati notificati dell'accaduto anche coloro i quali dati bancari si pensa possano essere stati violati. Adobe ha inoltre avviato le indagini sull'accaduto tramite l'aiuto delle autorità legislative e di importanti firme del settore.
L'analisi di questo caso ha mostrato quanto sia duttile una società operante in un contesto di mercato e organizzativo come quello di Adobe. L'agilità con la quale sono stati corretti gli errori che hanno portato all'incidente rappresenta proprio quell'assunto esposto in precedenza; in società come questa, il paradigma di risposta prevale nella gestione della sicurezza dell'organizzazione.

3.9 Caso otto: SK Communications

SK Communications è una società Sud Coreana, la quale si occupa di fornire servizi di server provider. Il suo prodotto più famoso è Nate, il quale nel 2003 si è fuso con CyWorld che è uno dei più famosi social network del paese.
Un po' come se fosse la Google Sud Coreana, SK Communications (per brevità da ora la chiameremo solamente SK) affronta le medesime problematiche di un qualsiasi altro gigante tecnologico. In analogia con il caso precedente, anche la struttura organizzativa di SK è

[12] Hash http://it.wikipedia.org/wiki/Hash
Sale (crittografia) http://it.wikipedia.org/wiki/Sale_(crittografia)

estremamente accentrata, costituita da poche sedi direzionali e con personale altamente specializzato. Anche in questo caso le decisioni vengono proposte, accettate e messe in pratica sostanzialmente nella stessa sede e, anche qui possiamo trovare una struttura informatica estremamente estesa, complessa e dinamica. Nel suo ruolo di service provider e gestore della gran parte dell'infrastruttura tecnologica operante nel paese, SK è inserita in un contesto estremamente innovativo e mutevole, di conseguenza pieno di pericoli. Data questa particolare struttura organizzativa e il contesto di mercato operante, anche in questo caso i dirigenti responsabili della sicurezza informatica saranno di fondamentale importanza per garantire il corretto svolgimento dei servizi offerti. Questi, oltre che garantire il corretto isolamento dell'infrastruttura da possibili attacchi esterni, devono soprattutto concentrarsi nel proteggere in profondo tutte le aree della struttura maggiormente a rischio e, devono essere pronti a reagire immediatamente sia alle nuove che alle più vecchie vulnerabilità. Devono garantire inoltre la disponibilità, integrità e riservatezza dei dati sia in transito che archiviati. In qualità di service provider infatti, la società maneggia miliardi di dati ogni anno e, per garantire il rispetto delle tre proprietà dei dati sopra citate deve essere effettuata una perfetta analisi dei rischi. Questa però è limitativo. Data l'elevata complessità tecnologica che viene utilizzata e, dato il settore in cui l'azienda opera, risulta molto rischioso basare la protezione delle infrastrutture e dei dati in transito interamente su misure preventive data la variabilità e l'imprevedibilità con cui questi rischi vengono corsi. Chiariti questi aspetti, possiamo affermare che anche in tale realtà, come in Adobe, la gestione dei rischi informatici sarà maggiormente sbilanciata sulla risposta che sulla prevenzione.

Anche la struttura fisico/tecnica necessita di essere impeccabile e, come nel caso precedente, deve essere posta particolare attenzione alla protezione dell'IT security (che secondo il TFI model si suddivide nella sicurezza dei computer e delle comunicazioni). Per quanto riguarda gli aspetti formali e informali invece, dovranno essere adottate le stesse misure di tutti i casi visti in precedenza. Per quanto riguarda l'aspetto formale, vi è la necessità di aderire a tutte quelle norme e quegli standard che in qualche modo possano aumentare il grado di sicurezza. Anche l'adozione di politiche interne è fondamentale, in quanto bisogna riuscire ad adattare le migliore pratiche di sicurezza con la struttura e l'organizzazione aziendale. Per quanto concerne l'aspetto informale, come chiarito nella teoria, vi è la necessità di riuscire a controllare tutte quelle variabili del comportamento umano he potrebbero trasformarsi in un pericolo per l'intera organizzazione. Detto questo passiamo in rassegna l'incidente avvenuto in SK e analizziamo quale sia stata la risposta a tale avvenimento.

Il 28 luglio 2011, SK Communications annuncia di esser stata vittima di un attacco informatico il quale ha sottratto 35 milioni di informazioni personali dei propri utenti. I dati compromessi erano relativi agli utenti del servizio CyWorld (il più grande social network della Corea del Sud) e Nate (un popolare portale web del paese). Tra il 18 e il 25 luglio 2011, gli hacker sono riusciti ad infettare più di 60 pc della società, riuscendo così ad ottenere l'accesso ai database dove vi erano archiviati i dati relativi agli utenti. Gli intrusi, per riuscire ad ottenere i permessi d'accesso ai computer aziendali e riuscire così ad installare il malware, si sono serviti dei canali di comunicazione esistenti tra SK e una società terza, fornitrice di software per SK. Dapprima sono stati compromessi i server di questa società terza, la quale forniva, oltre che i software necessari ad SK, anche delle pach d'aggiornamento. Una volta entrati in possesso dei server, gli hacker hanno sostituito il file d'aggiornamento con un trojan, il quale tramite il servizio di aggiornamento automatico di SK, venne scaricato su diverse macchine riuscendo così ad installarsi su queste. Una volta ottenuto il controllo dei computer, per gli hacker non fu difficile arrivare ai database.

I servizi di SK, erano così diffusi nel paese che, dopo tale evento, più della metà dei sud coreani avevano perso i propri dati personali. A permettere il furto, hanno quindi contribuito diversi fattori, tra cui sicuramente spicca l'abilità degli hacker. Questi sono riusciti a bypassare molteplici programmi di antivirus e sistemi di sicurezza interna senza essere in alcun modo notati e fermati. Tale incidente sottolinea appunto l'imprevedibilità di attacchi di questo genere e quindi di quanto sia difficile instaurare misure preventive che rendano minimi tali pericoli. SK, avendo adottato tutte le misure necessarie a garantire un ampio margine di sicurezza, non poteva prevedere un'intrusione di questo genere. Proprio per questo motivo ribadiamo ancora una volta che una società operante in un ambiente simile, debba necessariamente concentrarsi più sulla risposta che sulla prevenzione.

In risposta all'accaduto infatti, la società ha imposto la rimozione di ogni programma marchiato EST Soft, società che si era occupata dell'installazione e della manutenzione degli antivirus (il quale è stato ritenuto responsabile di non essere stato in grado di scovare il malware prima che questo fosse messo in funzione). Sono inoltre state aggiornate tutte misure di sicurezza, in modo da impedire che un simile evento possa verificarsi in futuro. La società si è inoltre presentata in giudizio per risarcire i danni ai consumatori danneggiati.

Chiaramente la società non può essere accusata sotto il punto di vista informale ma, avrebbe potuto adottare misure più stringenti sotto il punto di vista tecnico e formale. Per quanto riguarda il primo, si sarebbero potuti adottare ulteriori software capaci di individuare

programmi fraudolenti (come l' Host-Based Intrusion Prevent System, HIPS, visto in precedenza nel caso di JP Morgan) o, in alternativa misure preventive come una migliore scansione del programma scaricato. Sul lato formale invece, si sarebbero potute adottare politiche di sicurezza qualitativamente più efficienti, nel momento in cui avvenga uno scambio di informazioni con società terze (anche se si dovesse trattare di fornitori verificati), proprio come si sarebbe dovuto fare anche nel caso Target.
Tramite quest'analisi viene quindi confermato l'assunto che società operanti in contesti particolari (come quello di Adobe o SK), abbiano la necessità di concentrare maggiormente i propri sforzi su un gestione del rischio maggiormente di risposta.

3.10 Caso nove: Evernote Corporation.

Evernote è un'azienda indipendente privata con sede a Redwood City, California. E' stata fondata nel 2007 e i suoi prodotti raggiungono più di 100 milioni di utenti nel mondo.
Come Adobe ed SK Communications, anche Evernote fonda il proprio business sulla tecnologia ed in particolar modo sull'informatica. Come le altre due società appena studiate, anche in questo caso si può osservare una struttura organizzativa particolare, composta da poche sedi, un personale altamente qualificato e un'infrastruttura tecnologicamente molto complessa. Essendo però una società relativamente giovane ed essendo nata come una startup, il board di dirigenti non sarà certamente molto numeroso (a differenza di realtà come Adobe o JP Morgan) e magari, uno stesso soggetto potrebbe ricoprire più di un ruolo chiave. In un'ottica di questo genere però, non bisogna dimenticare che l'azienda opera in un contesto di mercato ancora nuovo (quello delle applicazioni mobili) e quindi caratterizzato da innumerevoli pericoli i quali potrebbero decretarne la sua fine (ad esempio a seguito di un grave incidente, gran parte degli utenti potrebbero trasferirsi su un altro servizio simile, data la semplicità di compiere tali azioni offerta dal mercato delle app mobile). Basando l'intera attività su internet e sulla propria applicazione, possiamo evidenziare come Evernote non abbia un network estremamente esteso. La base tecnologica è pertanto composta principalmente dai computer, con le quali lavorano i dipendenti e dai database, dove vengono archiviati i dati raccolti tramite il servizio. Date le caratteristiche societarie e di mercato, per le argomentazioni affrontate in precedenza, possiamo affermare senza ombra di dubbio che

anche questa realtà debba confrontarsi con un approccio alla gestione del rischio maggiormente orientato verso la risposta. Questo perché, anche in questo caso i rischi vengono percepiti come imprevedibili e non misurabili, in quanto l'azienda opera in un contesto ancora inesplorato, e vede l'intera propria attività basarsi sull'informatica. Non essendo estremamente chiare le tipologie di rischi che una società come Evernote, fondata sul mondo delle app mobile possa affrontare, ogni qualvolta che si verifichi un incidente (sia diretto alle proprie strutture che non), vi è la necessità che si attivi il paradigma di risposta in modo tale da poter far tesoro di quanto accaduto e riuscire a prendere le giuste precauzioni. Chiaramente, come già ripetuto per altre realtà, questo non sta a significare che non debba esservi una qualche forma di prevenzione. Devono essere adottate tutte le misure necessarie a garantire la protezione delle infrastrutture da modalità di attacco già conosciute in passato in modo da garantire una sicurezza generale. In questo Evernote è sempre stata in prima linea per favorirne l'adozione delle migliori tecnologie presenti sul mercato, atte a contrastare attacchi di questo genere. Detto questo, possiamo passare a descrivere il fatto che nel marzo 2013 ha provocato la perdita di oltre 50 milioni di dati riferibili ad altrettanti utenti.

Purtroppo, date le notizie ufficiali e dalle indiscrezioni trapelate sui più autorevoli esperti del settore, non è dato sapere molto sull'accaduto, tranne per il fatto che il sistema di sicurezza, durante l'attacco ha scovato delle attività sospette che tentavano di accedere ai dati protetti. Tramite un comunicato, l'azienda ha immediatamente chiarito che nessun dato caricato sugli account dagli utenti è stato rubato o modificato e che non sia stato violato alcun dato riferibile a carte di credito/debito. Gli hacker però sono riusciti ad accedere ai database dove erano archiviate informazioni quali username, password criptate e indirizzi email. La società ha anche assicurato che le password erano state criptate adoperando le ultime tecnologie e che quindi sarebbe stato molto difficile per gli avventori risalire ai dati originali.

Nonostante gli aggressori non siano riusciti ad entrare in possesso di alcuni dati rilevanti (gli username e le password se in formato criptato sono inutilizzabili ai fini di una possibile violazione della privacy) questo caso fa emergere quanto sia fondamentale, per Evernote, far si che la propria immagine non venga scalfita a seguito di eventi di questo genere. Questa necessità è sottolineata dal fatto che in Evernote, la sicurezza è posta sempre ai massimi livelli infatti, oltre ad aver adottato tutti gli standard di sicurezza generali (ad esempio utilizzando le ultime tecnologie in tema di criptazione utilizzando funzioni di hash+salt), la società è sempre in prima linea per proteggere i dati in loro possesso (lo dimostra il fatto che invita a denunciare al proprio team di supporto, qualsiasi sospetto di attività fraudolente) e per

promuovere l'adozione di standard di sicurezza sempre di maggior livello. Questo potrebbe far sembrare che l'azienda, dati gli sforzi nell'adozione di metodologie di sicurezza superiori, possa essere maggiormente sbilanciata verso una gestione del rischio di tipo preventivo invece che uno di risposta. A mio avviso ciò è fuorviante per varie ragioni. Innanzi tutto, per il contesto di mercato in cui opera. Come detto in precedenza, tale mercato ha ancora ampi spazi di sviluppo e, in un contesto tecnologico non maturo come lo è per l'appunto quello delle app mobile, i pericoli non ancora identificati, sono proporzionalmente elevati e dotati di una capacità di generare danni potenzialmente enormi. Il secondo motivo è collegato al primo ed è per il fatto che, una società di questo genere ha bisogno di essere immediatamente reattiva qualora si verifichino eventi di questo genere. Questo perché la struttura organizzativa e societaria non è ancora ben formata e, la clientela non può dirsi ancora totalmente fidelizzata (data anche la presenza di numerosi altri servizi di questo tipo). Oltre ciò, a mio avviso, bisogna tener presente che Evernote basa la propria forza su un sistema informatizzato e quindi altamente tecnologico che, per quanto visto sia nei casi precedenti, sia in teoria, necessita di un approccio alla gestione del rischio di tipo risposta. Quanto detto però conferma il fatto che si abbia la necessità di garantire la massima protezione delle strutture informatiche. Tornando più propriamente sull'accaduto, possiamo notare come non appena sia stata scoperta l'intrusione, siano state inviate a tutti gli utenti delle email contenenti un comunicato il quale faceva luce sull'accaduto e forniva ulteriori chiarimenti su cosa fosse o non fosse stato rubato. Oltre ciò, la società si è raccomandata, di modificare le proprie password (non solo quella di Evernote) in modo tale da non poter correre ulteriori rischi tramite nell'utilizzo di altri servizi informatici.

Sfortunatamente non sono state rilasciate ulteriori informazioni per quanto riguarda le tecniche di prevenzione e le politiche di sicurezza adottate pertanto non possiamo sapere se, a permettere l'intrusione sia stata la parte tecnica, formale o informale.

Avendo ora provveduto ad illustrare ed analizzare, sotto vari profili, nove dei ventitré casi riportati in questa tesi, siamo in possesso delle informazioni necessarie a poter definire uno schema generale che tenga conto degli aspetti comuni e delle divergenze riguardo alla modalità di approccio tra del paradigma di prevenzione e quello di risposta. Verranno utilizzati particolari termini di paragone capaci di raccordare le caratteristiche salienti di ognuno di questi casi.

3.11 Comparazione dei casi.

Tramite l'analisi appena condotta, possiamo raggruppare i casi in tre gruppi principali. Il primo, composto dalle prime tre società analizzate (TJX, Target, Home Depot), che potremmo definire "più tradizionaliste". Queste operano in ambienti relativamente stabili, caratterizzati da rischi per la maggior parte prevedibili, misurabili e ben conosciuti. Queste società sono anche caratterizzate da un basso livello tecnologico, proprio del loro core business, il quale, nella maggioranza dei casi consiste nelle strumentazioni necessarie alla conduzione dell'attività aziendale, come potrebbero esserlo tutte quelle strumentazioni presenti negli store e negli uffici amministrativi (computer, lettori ottici, casse, POS ecc.). I programmi software che vengono utilizzati quindi, sono per lo più utili alle attività proprie dell'impresa, come potrebbero esserlo dei software ERP[13] e/o CRM[14], con le quali l'azienda è in grado di compiere specifiche azioni come: la tenuta della contabilità, la gestione dei magazzini, la programmazione di campagne pubblicitarie e via discorrendo. Per le caratteristiche descritte nelle analisi sopra effettuate e, per i dati riassuntivi presentati in tabella possiamo pertanto affermare che questo primo gruppo sia caratterizzato da un approccio al rischio fortemente orientato alla prevenzione (dove però non vengono abbandonate completamente la strategie di risposta). Possiamo definire tale approccio come una "strategia fortemente preventiva" e rappresentarla tramite la seguente figura:

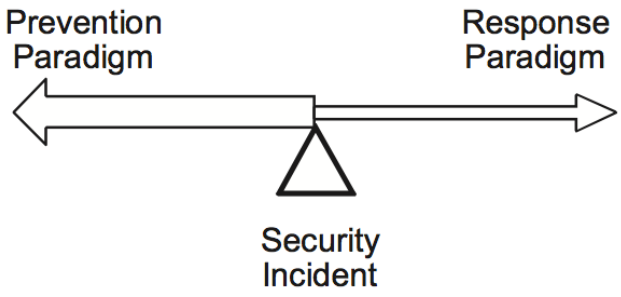

Figura 3.1 Bilanciamento strategico orientato alla prevenzione. [1]

[13] Enterprise resource planning http://it.wikipedia.org/wiki/Enterprise_resource_planning
[14] Customer relationship management http://it.wikipedia.org/wiki/Customer_relationship_management

Un secondo gruppo è invece composto dalle successive tre società (JP Morgan, HPS, eBay). Queste operano in ambienti meno stabili delle precedenti, in quanto l'integrazione delle comunicazioni e i nuovi processi d'informazione sviluppati attraverso internet (come potrebbero esserlo i nuovi servizi di cloud computing) fa si che tali società siano facili bersagli di attacchi informatici. Nonostante forniscano servizi "tradizionali" (prestazione di servizi finanziari e vendita di beni), l'evoluzione tecnologica del settore, ha creato la necessità di una forte implementazioni delle infrastrutture IT (nel caso di eBay e HPS queste sono essenziali) rendendole quindi molto complesse e geograficamente molto estese (basti pensare che queste società offrono servizi in quasi tutto il mondo). Questa crescita tecnologica, richiesta dal mercato, ha portato tali aziende a doversi interfacciare con rischi sempre meno prevedibili e misurabili, data la rilevanza e il numero dei dati da queste detenuti. Chiaramente sussistono ancora dei rilevanti rischi propri di business come questi e quindi misurabili e prevenibili. Questi potrebbero essere ad esempio, una truffa ben escogitata, uno scorretto comportamento di un dipendente o, ad esempio nel caso di JP Morgan un attacco fisico alle proprie filiali. Date quindi tutte le analisi effettuate durante la presentazione dei casi e, i dati riassuntivi della tabella, possiamo affermare come questo gruppo sia in una posizione intermedia tra una strategia preventiva e una di risposta. Possiamo definirla come una "strategia bilanciata" e rappresentarla attraverso la seguente figura:

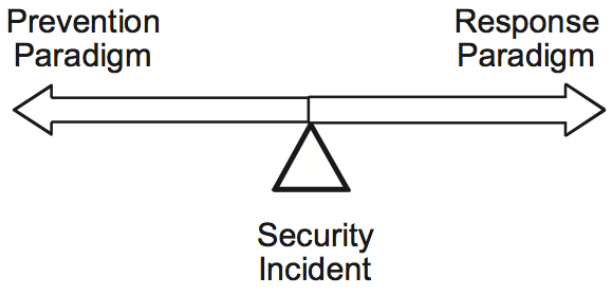

Figura 3.2 Bilanciamento equo tra prevenzione e risposta. [1]

Un terzo ed ultimo gruppo è invece composto dalle altre società analizzate (Adobe, SK Communications, Evernote). In questo caso, tutte operano in un settore estremamente volatile, dove le novità sono all'ordine del giorno e dove sono frequenti dei profondi cambiamenti nelle tecnologie utilizzate. Non è quindi possibile avere una sorta di stabilità in un contesto

simile. Il fatto che queste aziende operino in un settore come questo e, dato l'enorme contenuto tecnologico dei loro business, si vede necessaria l'adozione di un approccio alla gestione dei rischi decisamente di tipo risposta. In un tale contesto, difficilmente gli incidenti vengono ripetuti più volte allo stesso modo (a parte naturalmente nel caso di incidenti derivanti ad esempio da calamità naturali) e questo fa si che non sia possibile adottare misure preventive capaci di fronteggiare minacce di questo genere. Come abbiamo visto sopra, queste aziende sono dotate di una enorme infrastruttura tecnologica, di un vastissimo network (specialmente nel caso di SK Communications) e di una vastissima disponibilità di dati relativi ad un altrettanto vastissimo parco clienti. Queste caratteristiche fanno si che gli attacchi siano prevalentemente di tipo APT o comunque mirati ad ottenere informazioni rilevanti. Questo approccio prevalentemente di tipo di risposta non esclude delle forme di prevenzione agli attacchi, anzi in tali organizzazioni sono adottate tecniche di protezione molto pervasive e gli standard di sicurezza minimi richiedono particolari caratteristiche. Proporzionando le due strategie però, possiamo affermare che l'approccio prevalente è quello di tipo di risposta e può essere illustrato tramite la seguente figura:

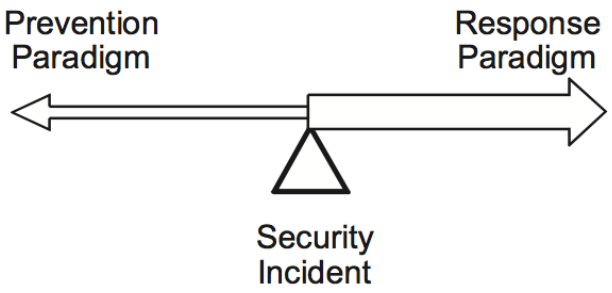

Figura 3.3 Bilanciamento strategico orientato alla risposta. [1]

Effettuate le comparazioni dei casi, possiamo ora agilmente sintetizzare gli aspetti salienti tramite l'utilizzo delle seguente tabella.

Tabella 3.1 Confronto tra i casi

	Livello di complessità tecnologica	Segmento di mercato operante	Tipologia di rischi assunti	Bilanciamento tra prevenzione e risposta
TJX	• Basso livello della tecnologia • Estensione del network limitata al processo di dati relativi alla gestione aziendale	• Vendita di capi d'abbigliamento e beni per uso personale	• I rischi sono per la maggior parte prevedibili e misurabili • Attraverso l'analisi dei rischi è possibile prevederne gran parte	• Vengono adottate maggiormente misure preventive derivanti dall'analisi dei rischi • La risposta viene ponderata in base alla tipologia di incidente subito
Target	• Basso livello della tecnologia • Estensione del network limitata al processo di dati relativi alla gestione aziendale	• Vendita di beni di consumo in generale	• I rischi sono per la maggior parte prevedibili e misurabili • Attraverso l'analisi dei rischi è possibile prevederne gran parte	• Vengono adottate maggiormente misure preventive derivanti dall'analisi dei rischi • La risposta viene ponderata in base alla tipologia di incidente subito
Home Depot	• Basso livello della tecnologia • Estensione del network limitata al processo di dati relativi alla gestione aziendale	• Vendita di prodotti per la casa	• I rischi sono per la maggior parte prevedibili e misurabili • Attraverso l'analisi dei rischi è possibile prevederne gran parte	• Vengono adottate maggiormente misure preventive derivanti dall'analisi dei rischi • La risposta viene ponderata in base alla tipologia di incidente subito
JP Morgan	• Alto livello della tecnologia • Estensione del network molto elevata. Vengono processati dati di natura economico-finanziaria di notevole importanza	• Servizi finanziari	• Alcuni rischi non sono prevedibili e misurabili • Non si può stabilire a priori la predicibilità e la persistenza di ogni rischio	• Vi è un generale bilanciamento tra prevenzione e risposta • Vengono adottate severe misure di prevenzione e la risposta si attiva contestualmente all'incidente permettendo così protezione ed innovazione

	Livello di complessità tecnologica	Segmento di mercato operante	Tipologia di rischi assunti	Bilanciamento tra prevenzione e risposta
HPS	• Alto livello della tecnologia • Estensione del network mediamente ampia. Vengono processati dati di natura economico-finanziaria	• Servizi di pagamento	• Alcuni rischi non sono prevedibili e misurabili • Non si può stabilire a priori la predicibilità e la persistenza di ogni rischio	• Vi è un generale bilanciamento tra prevenzione e risposta • Vengono adottate severe misure di prevenzione e la risposta è immediata, permettendo così protezione ed innovazione
eBay	• Alto livello della tecnologia • Estensione del network mediamente ampia. Vengono processati dati di natura economico-finanziaria	• Servizi di e-commerce	• La rapida evoluzione dell'ambiente forza l'azienda ad affrontare sempre nuovi rischi • Non si può stabilire a priori la predicibilità e la persistenza di ogni rischio	• Vi è un generale bilanciamento tra prevenzione e risposta • Vengono adottate severe misure di prevenzione e a seguito di un incidente si attiva l'intera struttura aziendale per aumentare l'innovazione e la protezione
Adobe	• Alto livello della tecnologia • Estensione del network mediamente ampia. Transitano per la maggior parte, dati relativi all'operatività aziendale	• Sviluppo software	• La rapida evoluzione dell'ambiente forza l'azienda ad affrontare sempre nuovi rischi • Attraverso l'analisi dei rischi è possibile ottenere solamente un quadro d'insieme sui rischi generalmente corsi	• Vi è una generale preferenza per un approccio di tipo risposta • La preferenza per la risposta fa si che a seguito di incidenti vi siano numerose innovazioni delle misure di sicurezza
SK Comm.	• Alto livello della tecnologia • Estensione del network estremamente ampia. Transitano dati di vario genere	• Gestione e sviluppo di infrastrutture informatiche • Servizi web	• La rapida evoluzione dell'ambiente forza l'azienda ad affrontare sempre nuovi rischi • Attraverso l'analisi dei rischi è possibile ottenere solamente un quadro d'insieme sui rischi generalmente corsi	• Vi è una generale preferenza per un approccio di tipo risposta • La preferenza per la risposta fa si che a seguito di incidenti vi siano numerose innovazioni delle misure di sicurezza

	Livello di complessità tecnologica	Segmento di mercato operante	Tipologia di rischi assunti	Bilanciamento tra prevenzione e risposta
Evernote	• Alto livello della tecnologia • Estensione del network estremamente ampia. Transitano dati di vario genere	• Servizi mobile	• La rapida evoluzione dell'ambiente forza l'azienda ad affrontare sempre nuovi rischi • Attraverso l'analisi dei rischi è possibile ottenere solamente un quadro d'insieme sui rischi generalmente corsi	• Vi è una generale preferenza per un approccio di tipo risposta • La preferenza per la risposta fa si che a seguito di incidenti vi siano numerose innovazioni delle misure di sicurezza

4. Conclusioni finali.

Dopo aver esaminato questi e numerosi altri casi (riassunti in appendice), possiamo definire che l'analisi qui esposta, è stata svolta con l'intento di fornire riscontri empirici su quanto teorizzato sul tema della gestione dei rischi in un contesto IT.

I casi sono stati analizzati dapprima sotto la lente della Actor – Network Theory (ANT), la quale ha cercato di far luce sulle complesse interazioni caratteristiche di ogni organizzazione. Successivamente ci si è concentrati sull'analisi della struttura e della complessità aziendale sotto l'occhio critico della Normal Accidents Theory (NAT), con la quale si è chiarito quale sia il livello di complessità tecnologico caratteristico di ogni organizzazione, per poi infine cercare di capire quali siano quelle realtà che potrebbero definirsi High Reliability Organizations (HRO). Nell'individuazione della struttura caratteristica di ogni società, si è fatto uso dello schema del TFI model, il quale è stato utile soprattutto nell'individuazione di quelle zone critiche che avrebbero potuto e che hanno dato luogo all'incidente. Infine, si è cercato di far luce su quale sia il bilanciamento tra prevenzione e risposta caratteristico di ognuna, date le differenti realtà in cui queste operano. In ultima analisi è stata svolta una comparazione cross dimensionale dei vari casi di studio, al fine di individuare quei gruppi caratterizzati dall'adozione di medesime proporzioni di prevenzione e risposta.

Concludendo, possiamo affermare che la nostra analisi ha preso in considerazioni molteplici elementi nel tentativo di definire quale sia il mix di prevenzione e risposta adottato da ognuna di queste realtà, qualora debbano affrontare rischi più o meno estesi. Gli elementi salienti che permettono di fornire tale definizione possono essere riassunti in:

- complessità tecnologica. Come abbiamo avuto modo di osservare, questa caratterizza ogni realtà aziendale, la quale la espone a rischi di diversa natura ed entità.
- posizione di mercato occupata. Come abbiamo visto, questa caratterizza sia la complessità tecnologica adottata, sia la rilevanza dei dati in possesso.
- numero e rilevanza dei dati in possesso. Più questi sono numerosi e sensibili, più richiedono una forte protezione. Allo stesso modo però, possono essere maggiormente un bersaglio per eventuali hacker che vogliano entrarne in possesso.

Queste caratteristiche sono quindi utili a poter giungere alla conclusione che specifiche caratteristiche, in specifiche realtà, concorrono a favorire differenti gradi di bilanciamento tra prevenzione e risposta verso quei pericoli che potrebbero minare la stabilità e l'operatività della società.

5. Appendice

Sono qui riportati i dati riassuntivi riguardanti tutti i data breach presentati nel capitolo precedente assieme ad altri che sono stati analizzati e riassunti nelle specifiche schede al fine di ottenere ulteriori conferme a quanto esposto sopra.

Caso uno. [20], [21], [22], [23], [24]

Nome: Adobe Systems Inc.

Descrizione società[15]: La Adobe Systems Inc. è una software house statunitense con sede principale a San Jose in California, nota soprattutto per i suoi prodotti di video e grafica digitale.

Descrizione fatto: Nell'ottobre 2013, un gruppo di hacker è riuscito a penetrare nei database dell'azienda rubando milioni di dati criptati, incluse password e altre credenziali d'accesso. Successivamente i dati comparvero online attraverso due file di dimensioni differenti, uno contenente i dati criptati e l'altro con i record in chiaro. Tutto ciò ha evidenziato come la metodologia utilizzata per la criptazione dei dati non fosse adeguata.

Quando: ottobre 2013.

Cosa è stato colpito: Database dei clienti.

Tipologia di dati rubati: Credenziali di accesso (ID e password), numeri di carte di credito e relativi dati.

Numeri: Inizialmente si pensava fossero stati rubati 38 milioni di dati utente. Successivamente si scoprì che invece erano 150 milioni.

Costo stimato: Non dato.

Prevention paradigm: Il metodo di criptazione adottato da Adobe, si è rilevato insufficiente. Questo non è riuscito a garantire la protezione dei dati archiviati, causando così gravi danni ai clienti i quali corrono/hanno corso il rischio di subire accessi non autorizzati sui propri conti bancari o in altri siti dove venivano utilizzate le medesime credenziali d'accesso.

15 Adobe Systems http://it.wikipedia.org/wiki/Adobe_Systems

Response paradigm: Come precauzione, Adobe ha immediatamente resettato le password dei propri clienti. La società ha così inviato delle email di notifica contenenti le istruzioni per effettuare il cambio di password. Nella email erano contenuti anche delle best-practice su come aumentare la propria sicurezza sul web. Sono stati avvisati dell'accaduto anche coloro i quali dati bancari si pensa possano essere stati rubati. Sono state inviate delle comunicazioni contenenti le procedure da seguire per proteggersi da eventuali furti sulle proprie carte di credito/debito. Adobe continua a lavorare sull'accaduto anche tramite l'aiuto di società esterne. E' stato avvisato anche la federal law enforcement per chiedere assistenza durante l'investigazione.

Technical: Nessun aspetto da evidenziare.

Formal: Per garantire la protezione dei propri dati, Adobe non ha utilizzato le ultime tecnologie di criptazione. I dati non erano criptati tramite una procedura detta hash+salt. Questa garantisce una forte protezione contro eventuali intrusioni, dal momento che i dati non solo vengono criptati tramite una funzione di hash ma, durante la fase di calcolo, viene aggiunta una stringa casuale di codice (chiamata "salt") in modo da ottenere un testo più articolato, con una stringa casuale e di conseguenza un codice hash finale maggiormente sicuro.

Informal: Nessun aspetto da evidenziare.

Caso due. [4]

Nome: TJX Companies, Inc.

Descrizione società[16]: TJX Companies è una società Americana che si occupa di abbigliamento e prodotti per la casa con sede in Framingham, Massachusetts. Sostiene di essere la più grande compagnia di abbigliamento e prodotti per la casa degli Stati Uniti. La società è un'evoluzione della catena Zayre, fondata nel 1956 il quale attraverso delle acquisizioni e dei distaccamenti è arrivata, nel 1988 a diventare TJX Companies. La società controlla altre marche d'abbigliamento e beni per la casa, come ad esempio: T.J. Maxx, Marshalls, Winners, HomeSense, HomeGoods, A.J. Wright, Bob's Stores, and T.K. Maxx.

Descrizione fatto: Nel 2005, un gruppo di hacker, sfruttando delle debolezze della rete di sicurezza WLAN, riuscirono ad intercettare i dati in transito in alcuni negozi di TJX. Gli

16 TJX Companies http://en.wikipedia.org/wiki/TJX_Companies

hacker si erano posizionati fuori dai negozi (in particolare quello di Marshall in St. Paul, Minnesota) e con una particolare antenna, per due giorni consecutivi, sono riusciti a catturare l'intero traffico in transito nel wireless network dello store, assicurandosi che nessuno avesse notato nulla. Dopo ciò, con i dati in loro possesso riuscirono a rompere il codice di sicurezza WEP del negozio riuscendo così ad ottenere l'accesso ad un gran numero di dati, tra cui le transazioni effettuate e i relativi dati delle carte di credito utilizzate per i pagamenti. Successivamente, nella seconda metà del 2006, i ladri riuscirono ad arrivare ai database principali della società ottenendo così, oltre che delle informazioni vitali per la società, anche un'enorme mole di dati dei clienti. Si pensa che siano più di 45 milioni i dati rubati.

Quando: 2005-2006-2007

Cosa è stato colpito: Inizialmente è stata colpita la rete wireless del negozio Marshall, il quale ha dato accesso ai dati presenti nei computer del negozio. Successivamente gli hacker sono riusciti ad arrivare alla base operativa dell'intero gruppo, ottenendo così un numero di dati nettamente maggiore.

Tipologia di dati rubati: Dati di carte di credito, credenziali d'accesso ai conti correnti, dati personali.

Numeri: Più di 45,7 milioni di dati furono rubati.

Costo stimato: Più di 300 milioni di dollari tra costi diretti e indiretti.

Prevention paradigm: La struttura di sicurezza della società, al momento della prima aggressione era molto debole. Venivano usati sistemi di cifratura obsoleti (quali era il sistema Wired Equivalent Privacy WEP) e ciò ha fatto sì che gli intrusi, una volta capito il metodo di sicurezza utilizzato, non impiegassero molto ad invadere la rete.

Response paradigm: Dopo esser venuti a conoscenza dell'intrusione, il management ha deciso di adottare immediatamente il più sicuro protocollo di sicurezza WPA (Wifi Protected Access) e successivamente sono scattate le indagini sull'accaduto. Dopo aver appreso l'entità del danno, si è deciso di avvertire la law enforcement agency e, solamente qualche tempo dopo, il 17 gennaio 2007 è stata resa pubblica la notizia. Questa ha portato ad ulteriori indagini esterne sull'accaduto, le quali hanno messo in luce ulteriori problemi di sicurezza.

Technical: L'area della Technical security che ha fatto sì che si perdesse la confidenzialità dei dati è quella della Communication Security. Come sopra citato, le misure di sicurezza adottate erano obsolete e, nonostante il CIO Paul Butka avesse già menzionato questo handicap e suggerito l'adozione di standard più sicuri (quello WPA), si è preferito evitare

ulteriori costi e rimandare l'aggiornamento ad una data futura, esponendo così la società al rischio che poi ha effettivamente corso.

Formal: Per quanto riguarda gli elementi formali del security management, bisogna sottolineare che già nel 2005 la compagnia non rispettava 9 dei 12 requisiti di sicurezza imposti dai nuovi standard PCI DSS.

Informal: Nessun aspetto da evidenziare.

Caso tre. [5], [25]

Nome: Target Corporation.

Descrizione società[17]: Target Corporation è una società di vendita al dettaglio americana, fondata nel 1902 e con sede in Minneapolis, Minnesota. Con più di 366.000 dipendenti è la seconda società di questo genere negli Stati Uniti (Walmart è la prima).

Descrizione fatto: Gli hacker sono riusciti ad ottenere l'accesso ai dati attraverso più fasi. Dapprima hanno ottenuto informazioni (attraverso Google) circa il modo in cui Target si relazionava con i propri fornitori. Appreso ciò, attraverso un documento reso pubblico da Microsoft, sono venuti a conoscenza circa l'infrastruttura tecnica di Target, inclusi importanti dettagli sul funzionamento dei POS. Successivamente venne inviata un'email contenente un virus ad un fornitore della società, due mesi prima dell'attacco, il quale una volta istallato sulle macchine, funzionò come ponte di collegamento tra gli hacker e Target. Creato questo ponte, per gli hacker non fu difficile infiltrarsi nel network. Una volta entrati nel sistema infatti, riuscirono ad ottenere l'accesso al sistema di gestione dei POS, istallando così un malware (invisibile agli antivirus) che si diffuse velocemente su tutti i POS della società. Il software istallato, era capace di memorizzare i dati delle carte di credito ogni qualvolta queste venivano strisciate e, attraverso un particolare canale di comunicazione, i dati venivano inviati agli hacker.

Quando: Dicembre 2013

Cosa è stato colpito: Dati contenuti nei Point Of Sales (POS) di circa 2000 negozi.

Tipologia di dati rubati: Nomi dei clienti, numeri e codici di sicurezza delle carte di credito/debito.

Numeri: Oltre 40 milioni di dati di carte di credito riferibili ad oltre 70 milioni di clienti.

[17] Target Corporation http://en.wikipedia.org/wiki/Target_Corporation

Costo stimato: I costi furono altissimi. Devono considerarsi tra i costi diretti sostenuti, gli oltre 200 milioni di dollari che le banche dovettero rimborsare ai propri clienti. Tra i costi indiretti devono considerarsi il licenziamento di un gran numero di dipendenti di alto livello, tra i quali figurano il CEO e il CIO, il gran numero di cause legali avviate contro la società (circa 140) e il calo dei profitti del 46% verificatosi solo nel quarto quadrimestre del 2013.

Prevention paradigm: Il caso Target è emblematico. Nonostante tutte le misure di sicurezza adottate (come ad esempio la conformità alle normative di sicurezza dei POS) e la grande attenzione posta ai dati maggiormente sensibili, gli hacker sono comunque riusciti a penetrare all'interno del sistema. Anzitutto vi erano lacune laddove Target veniva in contatto con i propri fornitori attraverso il sistema telematico. Questo deriva dal fatto che, i responsabili della sicurezza, hanno preferito concentrare i propri sforzi per proteggere direttamente i dati sensibili archiviati e non tanto il "perimetro" della struttura. Questa mancanza ha fatto sì che non fosse difficile per gli hacker, penetrare nel sistema. Altra importante lacuna vi è nel sistema di sicurezza dei POS. Gli hacker sono riusciti ad istallare il malware all'interno dei dispositivi, il quale registrava ed inviava i dati delle carte di credito ai criminali. Questo non sarebbe dovuto accadere. Si sarebbero dovuti utilizzare metodi più efficaci, quali ad esempio un sistema di whitelisting, il quale garantisce l'istallazione e l'esecuzione dei soli programmi accettati e contenuti nella whitelist.

Response paradigm: Dopo l'intrusione, si è provveduto immediatamente ad analizzare il danno assicurandosi di adottare tutte le misure di sicurezza necessarie. La società ha collaborato sia con le autorità giudiziarie che con società private, in modo da far luce sul caso. Questo evento, ha fatto sì che venissero fuori ulteriori lacune, oltre che proprie di Target, anche degli standard di sicurezza utilizzati.

Technical: I problemi di sicurezza non erano solamente legati ad aspetti software, ben sì anche hardware. Si sarebbe potuto evitare il tutto ad esempio adottando tecnologie come l'Hardware Security Module (HSM), il quale avrebbe assicurato l'istallazione di soli moduli dotati di un particolare codice di sicurezza. Ulteriori metodi (come il Tamper Resistant Security Module, TRSM) sarebbero potuti essere implementati per proteggere il POS operating system memory memorizzando i dati criptati nell'hardware e non in un software. Ancora, si sarebbe potuto utilizzare il Point-to-Point Encryption (P2PE), il quale avrebbe aggiunto un'ulteriore grado di sicurezza.

Formal: La società era in regola con gli ultimi standard di sicurezza ma, presentava alcune lacune nelle politiche di sicurezza interne.

Informal: Per quanto riguarda le carenze del comportamento umano, nei sistemi di comunicazione, la colpa la si può dare solamente al fornitore di Target (Fazio Mechanical), il quale non adottando la normale diligenza nell'accettarsi della fonte dell'email contenente il malware, ha fatto sì che gli hacker ottenessero un pivot point da cui gestire l'intera operazione.

Caso Quattro. [6], [26], [27]

Nome: Heartland Payment Systems Inc.

Descrizione società[18]: Heartland Payment Systems (HPS) è una società che si occupa di pagamenti elettronici. Fondata nel 1997 da Robert O. Carr, con sede in Princeton, New Jersey, è una delle più grandi società del settore.

Descrizione fatto: Per infiltrarsi all'interno del sistema di HPS, gli hacker hanno utilizzato una metodologia di hacking detta SQL injection sfruttando così un bug del sistema. Questo, non era mai stato identificato prima, ne tramite i controlli periodici, ne tramite controlli campionari. Una volta che gli hacker sono riusciti ad invadere il sistema, hanno istallato un programma di sniffing, capace di raccogliere informazioni su: dati di carte di credito, nominativi dei clienti e tutti i dati mossi attraverso il sistema HPS.

Quando: 2007-2008-2009

Cosa è stato colpito: Network societario.

Tipologia di dati rubati: Dati di carte di credito, nominativi clienti e altri dati gestiti attraverso il sistema HPS.

Numeri: 130.000.000 di dati rubati.

Costo stimato: 170 milioni di dollari furono associati ai costi diretti dell'accaduto. 20 milioni di questi furono rimborsati dalle assicurazioni.

Prevention paradigm: La società era in linea con tutti gli standard di sicurezza e aveva un sistemi di controlli interni molto efficiente. Gli hacker sono però riusciti a sfruttare un errore nella scritturazione del codice del programma di gestione del sistema di HPS senza che alcun programma di sicurezza abbia potuto dare l'allarme e fermare l'attacco. L'unico modo

[18] Heartland Payment Systems http://en.wikipedia.org/wiki/Heartland_Payment_Systems

per poter prevenire un attacco di questo genere sarebbe quello di riuscire scrivere un programma privo di falle (cosa praticamente impossibile).

Response paradigm: Verificatosi l'incidente, HPS modificò il proprio atteggiamento in termini di sicurezza, difatti adottò politiche estremamente pervasive in termini di sicurezza, realizzando ad esempio, un sistema end-to-end encryption atto a garantire la massima sicurezza dei dati ogni qual volta avvenga un pagamento. La criptazione avviene in ogni momento della transazione, dal momento della "strisciata" sul terminale, a quando si riceve l'accettazione finale. Inoltre HPS, si è impegnata a realizzare, assieme ad una società Taiwanese, un nuovo modello di POS estremamente sicuro (dotato di un sistema di criptazione hardware). Oltre ciò, la società si è impegnata nell'istituzione del gruppo FS-ISAC, volto a promuovere lo scambio di informazioni: l'FS-ISAC Payment Processors Information Sharing Council. Può quindi dirsi che l'incidente abbia scosso profondamente Heartland.

Technical: Nulla da rilevare.

Formal: Nonostante HPS aderisse ai vari protocolli di sicurezza, questi si sono rivelati insufficienti nell'evitare la perdita di informazioni. Questo può significare che tali standard di sicurezza rappresentano solamente il livello minimo necessario. Le società (come avrebbe dovuto fare HPS prima dell'intrusione) dovrebbero instaurare un sistema di controlli interni estremamente minuzioso, proprio per scongiurare qualsivoglia tipo di intrusione.

Informal: Nulla da rilevare.

Caso cinque [8], [28], [29], [30]

Nome: Sony Corporation.

Descrizione società[19]: Sony Corporation è un gruppo economico giapponese, tra i primi cento al mondo per fatturato e presente nei settori dell'elettronica di consumo, della comunicazione e dei servizi finanziari.

Descrizione fatto: il 19 aprile 2011, il Playstation Network di Sony, è stato bersaglio di un attacco informatico il quale ha permesso l'ottenimento da parte degli hacker di 77 milioni di record. Risulta pertanto uno degli attacchi più eclatanti nel suo genere. Questo è stato messo in atto attraverso più fasi e tramite l'utilizzo di diverse metodologie di hacking. Inizialmente

[19] Sony http://it.wikipedia.org/wiki/Sony

gli hacker hanno preso di mira il sito del servizio, riuscendo a sospenderlo momentaneamente. Successivamente si sono serviti di un'SQL injection per infiltrarsi all'interno dei database ed ottenere così l'ingente bottino.

Quando: Aprile 2011

Cosa è stato colpito: Play Station Network (PSN)

Tipologia di dati rubati: Informazioni personali inclusi dati di carte di credito.

Numeri: 77 milioni di accounts violati

Costo stimato: Più di 171 milioni di dollari. Le azioni Sony sono scese da 36.36$ dell'11 gennaio 2011 a 24.28$ per azione il 20 giugno 2011.

Prevention paradigm: L'attacco, rivendicato dal gruppo Lulz, aveva lo scopo di dimostrare quanto fosse debole il sistema di sicurezza della compagnia. Attraverso alcune ricerche condotte dopo l'attacco, è risultato che vi erano problemi di sicurezza già nel sito web, il quale poteva essere facilmente violato.

Response paradigm: Una volta venuti a conoscenza dell'intrusione, gli ingegneri Sony hanno temporaneamente sospeso il servizio in modo da fermare l'intrusione e il flusso di dati in uscita. Contestualmente sono state assunte delle società di sicurezza informatica in modo tale da far scattare le indagini. Una volta effettuate, venne rilasciata una dichiarazione pubblica dove veniva affermato che probabilmente a seguito dell'attacco potrebbero essere stati rubati dei dati riferibili ai clienti. Successivamente, venne varata una riorganizzazione dell'intero sistema di sicurezza del PSN, in modo da garantire una maggiore affidabilità e sicurezza.

Technical: Nulla da rilevare.

Formal: Non era stata adottata alcuna misura di sicurezza necessaria ad ottenere un livello accettabile di sicurezza all'interno del sistema. Il PSN aveva policy di sicurezza molto limitate ed infatti era possibile ottenere l'accesso a numerose aree semplicemente sfruttando errori di progettazione banali anche attraverso il sito web. Il più grande errore di Sony è stato a livello manageriale. L'intero sistema di sicurezza e la struttura del PSN hanno fatto sì che vi fossero numerose vie di accesso per un qualsiasi intruso.

Informal: Nulla da rilevare.

Caso sei [31], [32], [33], [34], [35]

Nome: Epsilon

Descrizione società[20]: Epsilon è una società americana attiva in diversi settori tra cui: servizi di marketing (raccolta di dati di marketing, email marketing ecc.), sviluppo web, consulenze strategiche, email service provider ed altro. La società è il più grande permission-based email marketing provider del mondo ed invia oltre 40 miliardi di email all'anno per conto di più di 2500 clienti. Nel 2011 è stata acquisita da Aspen Marketing Services.

Descrizione fatto: Nel marzo del 2011 la società ha subito un'intrusione nei propri database, dalla quale sono stati sottratti numerosi indirizzi email relativi a circa il 2% dei clienti di Epsilon (tra cui figurano tra questi: Best Buy, Citibank, Walt Disney Company)

Quando: Marzo 2011

Cosa è stato colpito: Il database responsabile della gestione del servizio di email marketing provider.

Tipologia di dati rubati: Nomi ed indirizzi email dei clienti delle società clienti di Epsilon. Gli intrusi non hanno avuto accesso ad altri dati come: credenziali d'accesso, dati di carte di credito e qualsiasi altro tipo di dato personale.

Numeri: L'incidente ha riguardato circa il 2% dell'intero parco clienti della società

Costo stimato: Le ripercussioni dirette dell'attacco superano i 400 milioni di dollari ma, gli analisti ritengono che nel worst case scenario il costo potrebbe raggiungere i 4 miliardi.

Prevention paradigm: Informazioni non sufficienti.

Response paradigm: Il 31 marzo, Epsilon dichiara di aver subito un'intrusione e, contestualmente molte delle sue società clienti, avvertirono i propri clienti del fatto che i loro dati (solamente gli indirizzi email e i relativi nominativi) potrebbero esser stati sottratti durante l'attacco. Fortunatamente non sono stati compromessi altre tipologie di dati, pertanto si sono limitati a notificare la clientela dell'accaduto e metterla in guardia verso possibili attacchi di phishing. Dopo aver attivato il protocollo di sicurezza pronto a gestire e aver avviato delle indagini interne, il fatto è stato anche denunciato all'US Secret Service e altre agenzie governative.

Technical: Dati non sufficienti.

Formal: Dati non sufficienti.

[20] Alliance Data http://en.wikipedia.org/wiki/Alliance_Data

Informal: Dati non sufficienti.

Caso sette [36], [37], [38], [39]

Nome: CardSystem Solution Inc.

Descrizione società[21]: CardSystem Solutions, era una società attiva nell'invio e nella ricezione di pagamenti effettuati tramite carte di credito. Il 9 dicembre 2005 viene acquistata da Pay By Touch, il quale fallirà il 19 marzo 2008.

Descrizione fatto: Nel maggio 2005, alcuni hacker, riuscendo ad intrufolarsi all'interno dei database aziendali, sono riusciti ad ottenere un elevato numero di credenziali d'accesso agli account di numerose compagnie di carte di credito. Non si è a conoscenza di come gli hacker siano riusciti ad entrare all'interno dei computer ma, è stato solamente detto che questi hanno un'SQL injection che gli ha permesso di ottenere gli accessi necessari. Inoltre, non è stato dichiarato per quanto tempo gli abbiano avuto la disponibilità del sistema. Dopo la scoperta dell'accaduto, i due più grandi player mondiali nel settore delle carte di credito (Visa e MasterCard) si sono adoperate a fondo per far luce sull'accaduto in quanto molti di quegli account erano gestiti proprio da loro. Già dal 2004 le due società hanno optato per fare in modo che chiunque entrasse in contatto con informazioni sensibili di carte di credito adottasse specifici standard di sicurezza (i PCI standard per l'appunto). Nel corso delle indagini, si è venuto a scoprire che la società non era in linea nell'adozione degli standard proposti dai PCI DSS.

Quando: 2005

Cosa è stato colpito: Database aziendali.

Tipologia di dati rubati: Account di carte di credito e i relativi dati di accesso.

Numeri: Oltre 40 milioni di account di carte di credito, tra cui 22 milioni di Visa, 14 di MasterCard e 1,6 di American Express.

Costo stimato: Non dato.

Prevention paradigm: Ciò che ha permesso agli hacker di intrufolarsi all'interno dei database di CardSystem lo si può ricollegare all'adozione di scarse policy di sicurezza sia interne che esterne nonostante la gestione di dati estremamente sensibili.

---

21 CardSystems Solutions http://en.wikipedia.org/wiki/CardSystems_Solutions

Response paradigm: Una volta venuti a conoscenza dell'intrusione, la società ha denunciato l'accaduto all'FBI e all'associazione delle carte di credito. Effettuate le indagini di dovere, sono state immediatamente adottate tutte le misure necessarie a garantire un maggior livello di sicurezza.

Technical: Nulla da rilevare.

Formal: Ciò che ha consentito l'intrusione può ricondursi in due principali fattori:

1. Le scarse policy di sicurezza interna.
2. La non completa aderenza agli standard PCI DSS.

Informal: Nulla da rilevare.

Caso otto [7], [40], [41]

Nome: J.P. Morgan Chase & Co

Descrizione società[22]: J.P. Morgan Chase & Co. è una società finanziaria con sede a New York, ed è leader nei servizi finanziari globali. Attualmente serve più di 90 milioni di clienti.

Descrizione fatto: Tutto ebbe inizio nel giugno 2014 quando il computer di un dipendente fu infettato da un virus e gli rubò delle credenziali d'accesso. Una volta collegatosi alla rete aziendale, l'hacker fu capace di fruttare questo punto come pivot point per entrare nel network aziendale. Da questo punto, è stato possibile, tramite un virus disegnato ad hoc, penetrare i più alti livelli di sicurezza e riuscire a controllare oltre 90 server societari. Per evitare di essere scoperti, gli hacker hanno fatto in modo di sottrarre informazioni poco alla volta nell'arco di molti mesi. Il breach non sarebbe stato scoperto se nell'agosto dello stesso anno non fosse stato violato anche uno dei loro siti internet. Avviate le indagini su quest'ultimo incidente si è venuto a scoprire che la società era caduta vittima di un attacco diretto ai propri database. Tutto ciò nonostante la società investa annualmente oltre 230 milioni di dollari in cyber security impiegando oltre 1000 specialisti.

Quando: 2014

Cosa è stato colpito: Database aziendali, computer dei dipendenti e network aziendale.

Tipologia di dati rubati: Nominativi, indirizzi di residenza, numeri telefonici, indirizzi email di 76 milioni di famiglie e 7 milioni di piccole imprese

Numeri: 83 milioni di dati rubati

[22] JPMorgan Chase http://it.wikipedia.org/wiki/JPMorgan_Chase

Costo stimato: Non dato

Prevention paradigm: Nonostante gli ingenti investimenti in sicurezza informatica, anche JP Morgan è caduta vittima di un attacco di questo genere. Come è naturale pensare, è impossibile essere protetti al 100% da questo tipo di pericoli (l'unico modo sarebbe quello di non dotarsi di un sistema informatico) e, in questo ambito, JP Morgan è stata attaccata su due fronti. Uno è quello umano, ovvero gli intrusi hanno ottenuto il primo contatto con il network aziendale infettando un dipendente tramite un'email. L'altro è quello tecnico-formale relativo ai permessi attribuiti ai dipendenti e alla struttura informatica.

Response paradigm: Dopo aver subito l'attacco, JP Morgan ha organizzato un business control group composto da una dozzina di esperti in cyber security per sopperire a tali mancanze. Fortunatamente il danno si è esteso solamente agli indirizzi email, recapiti telefonici e indirizzi di residenza, senza intaccare credenziali d'accesso ai conti bancari ed altro. Ovviamente appena si è venuti a conoscenza dell'accaduto la società ha dato il via a scrupolose indagini sia tramite esperti privati che tramite l'aiuto dell'FBI.

Technical: Un modo sicuramente efficace per contenere attacchi di questo genere, è sicuramente quello di suddividere il network interno in segmenti e non avere un unico grande blocco dove chiunque (o quasi) può ottenere qualsivoglia informazione. L'idea è quella di restringere i permessi d'accesso alle sezioni critiche solamente a coloro che effettivamente necessitano di tali risorse. Ad esempio il dipendente allo sportello non dovrebbe avere accesso alla piattaforma di controllo dei terminali o ancora, gli ingegneri che si occupano della sicurezza non dovrebbero aver accesso alle informazioni strategiche societarie e così via. Questo però non era quanto accadeva in JP Morgan dove, il dipendente che è stato preso di mira, era in possesso di maggiori permessi di quanti effettivamente avrebbe avuto bisogno. Esistono vari metodi che avrebbero sopperito a questa mancanza, uno di questi è il Network Access Control (NAC), il quale è in grado di rilasciare l'accesso al richiedente solo dopo aver scansionato la macchina nella ricerca di un possibile malware.

Formal: Nonostante JP Morgan fosse in linea con i vari standard di sicurezza generalmente imposti e nonostante spendesse un'ingente somma in cyber security (circa 250 milioni di dollari all'anno), i responsabili delle policy di sicurezza interna non hanno pensato che per entrare in possesso di determinati dati o strumenti fosse necessario un sistema di login ad hoc. Quello adottato era il classico username/password quando invece, sarebbe stato più opportuno adottare il metodo dell'autenticazione a due fattori il quale richiede una one-time password

(OTP) – fornita su un altro dispositivo (solitamente su dei token) – prima di permettere l'accesso alle informazioni riservate.

Informal: Il primo contatto con la società, è avvenuto tramite un virus installato sulla macchina di un dipendente. Non si hanno notizie ufficiali su come siano riusciti a compromettere il pc ma, molto probabilmente, questo è accaduto a causa di email phishing. Esistono numerosi metodi per scongiurare questo genere di attacchi ed uno di questi è, quello di tenere aggiornato il proprio antivirus e/o installate un Host-Based Intrusion Prevent System (HIPS) il quale ha un funzionamento simile. Oltre a misure tecniche però, è fondamentale anche che si adottino particolari policy di sicurezza atte ad evitare errori di questo genere, istruire i dipendenti sulle normali pratiche di sicurezza informatica, tenere corsi di ingegneria sociale.

Caso nove [9], [42]

Nome: eBay Inc.

Descrizione società[23]: eBay Inc. è un sito di aste on-line fondato il 6 settembre 1995 da Pierre Omidyar; in Italia è arrivato nel 2001 rilevando il sito iBazar. eBay è una piattaforma web (marketplace), di fatto molto simile ad un sito di e-commerce, che offre ai propri utenti la possibilità di vendere e comprare oggetti sia nuovi sia usati, in qualsiasi momento, da qualunque postazione Internet e con diverse modalità, incluse le vendite a prezzo fisso e a prezzo dinamico, comunemente definite come "aste online".

Descrizione fatto: L'intrusione è stata resa possibile grazie al furto di alcune credenziali d'accesso di un piccolo numero di dipendenti. Probabilmente erano state ottenute grazie ad uno spear-phishing email attack[24]. Una volta ottenuti i permessi d'accesso, gli hacker sono riusciti ad entrare nel sistema di eBay ed avere accesso ai database. Fortunatamente non è stato rubato nessun tipo di dato riferibile a carte di credito, in quanto questi erano memorizzati in database differenti (quelli di PayPal).

Quando: Febbraio-Marzo 2014.

Cosa è stato colpito: Dapprima i personal computer dei dipendenti poi, una volta ottenute le credenziali necessarie, si sono infiltrati nei database societari.

---

[23] eBay http://it.wikipedia.org/wiki/EBay

[24] spear phishing http://searchsecurity.techtarget.com/definition/spear-phishing

Tipologia di dati rubati: Nominativi clienti, indirizzi email, indirizzi di residenza, numeri telefonici, password criptate, date di nascita. Nessuna informazione finanziaria è stata rubata.

Numeri: 145 milioni di dati utente.

Costo stimato: Non dato.

Prevention paradigm: Il sistema di sicurezza interno era affidabile tanto che la causa dell'attacco non è stata identificata in una falla del sistema di sicurezza vero e proprio bensì in un errore umano. L'efficacia del sistema di sicurezza eBay è stato confermato anche dal fatto che gli hacker non sono riusciti ad ottenere alcuna informazione finanziaria dei clienti in quanto queste erano archiviate su un network differente e separato.

Response paradigm: Il comportamento di eBay all'attacco non fu certamente uno dei migliori in quanto i clienti non vennero avvisati dell'attacco se non solo due settimane dopo. Nulla fu scritto sulla pagina web ufficiale della compagnia, nessuna email fu spedita ai clienti e nessuna notifica fu attivata nemmeno quando i clienti effettuavano l'accesso al sito. Solo dopo queste due settimane i clienti vennero informati tramite un'email contenente informazioni riguardo l'intrusione, cosa è stato compromesso e delle best practice per scongiurare future perdite di dati. eBay sta collaborando con l'FBI e compagnie private per far luce sull'accaduto.

Technical: Nulla da evidenziare.

Formal: Nulla da evidenziare.

Informal: Come si evidenzia nella teoria di ICT, l'errore umano è la principale causa di eventi sconvenienti e talvolta catastrofici per un sistema informatico e ancora più per un'intera azienda. Questo perché mentre un qualcosa di artificiale, come potrebbe essere un sistema informatico, può essere teoricamente inattaccabile e controllabile al 100%, il comportamento umano funziona in maniera differente. Ognuno agisce con scopi e metodi differenti e questa è la causa principale della rischiosità dei comportamenti umani. Una conferma di questo assunto la fornisce il caso di eBay dove è stato per l'appunto un comportamento umano errato (l'essere stati adescati da email fraudolente) a causare la perdita di un'enorme quantità di dati. Questo rischio però fortunatamente può essere mitigato e ridimensionato tramite pratiche come quelle citate nel caso otto ovvero di training del personale su particolari tematiche di sicurezza, adozione di particolari protocolli da seguire nello svolgimento di alcune attività e così via.

Caso dieci. [10], [11], [43], [44]

Nome: Home Depot Inc.

Descrizione società[25]: Home Depot è un venditore al dettaglio statunitense di prodotti per migliorare, costruire e manutenere la casa. Ha la sua sede a Vinings, nella Contea di Cobb (Georgia) appena fuori da Atlanta. Home Depot impiega più di 355.000 persone e gestisce 2.164 Superstore distribuiti negli Stati Uniti, Canada, Messico e Cina. Attualmente è il più grande distributore di prodotti per la casa degli Stati Uniti, davanti al rivale Lowe's, e il secondo più grande distributore in generale degli Stati Uniti, preceduto solo da Wal-Mart.

Descrizione fatto: Nel settembre 2014, Home Depot afferma di aver subito un attacco informatico che le ha sottratto un'enorme quantità di dati estremamente riservati. Gli hacker sono riusciti a sviluppare un malware appositamente per il caso, capace di raccogliere dati sensibili dai POS (Point Of Sale). Il malware utilizzato non era mai stato identificato prima ed infatti era stato in grado di superare gli antivirus installati sulle macchine senza trovare alcun tipo di resistenza. Dapprima si credeva che gli hacker avessero ottenuto l'accesso ad informazioni come password e carte di credito/debito mentre successivamente, attraverso indagini approfondite, si è chiarito che sono stati rubati solo degli indirizzi email. La società ha quindi poi provveduto ad informare la clientela.

Quando: Settembre 2014

Cosa è stato colpito: L'attacco è stato effettuato dapprima tramite un malware, il quale è stato in grado di colpire i POS di svariati negozi, per poi arrivare ai database societari contenenti numerosi dati sensibili.

Tipologia di dati rubati: Indirizzi email dei clienti.

Numeri: 56 milioni di dati.

Costo stimato: L'intrusione potrebbe costare, nel peggiore dei casi, fino a 3 miliardi di dollari.

Prevention paradigm: Informazioni non sufficienti.

Response paradigm: Poco prima dell'attacco, Home Depot aveva già avviato delle procedure di upgrade dell'infrastruttura di sicurezza presente nei suoi stores agli inizi del 2014, la quale sarebbe dovuta terminare entro la fine dell'anno, per poi procedere con l'aggiornamento degli stores canadesi. Dopo l'accaduto però, il management ha optato per

[25] Home Depot http://it.wikipedia.org/wiki/Home_Depot

una più rapida conclusione dell'upgrade tanto che, a fine settembre tutti gli stores americani erano già stati aggiornati, mentre l'aggiornamento canadese sarebbe terminato entro i primi mesi del 2015.

Technical: Informazioni non sufficienti.

Formal: Sicuramente si può additare il sistema di sicurezza allora presente se l'attacco è andato a buon fine. Risultava essere insufficiente rispetto ai doveri che doveva assolvere, tant'è vero che il management aveva già messo in preventivo un imminente aggiornamento del sistema. Sicuramente però, se si fossero utilizzati dei sistema di sicurezza più profonda, (ad esempio tramite l'utilizzo di withelist, le quali non permettono l'esecuzione di programmi non presenti nella lista di quelli accettati) si sarebbe potuto scongiurare l'accaduto.

Informal: Informazioni non sufficienti.

Caso undici [45], [46], [47]

Nome: LivingSocial Inc.

Descrizione società[26]: LivingSocial è una piattaforma online che permette ai clienti di acquistare e condividere eventi in città. Con sede in Washington D.C., LivingSocial ha oltre 70 milioni di utenti registrati in tutto il mondo.

Descrizione fatto: Nell'aprile 2013 alcuni hacker sono riusciti ad ottenere degli accessi non autorizzati ai server di LivingSocial riuscendo così a rubare milioni di credenziali d'accesso come: nickname, password, email, date di nascita.

Quando: Aprile 2013

Cosa è stato colpito: Server e database societari. Fortunatamente non è stato possibile accedere ai database contenenti le informazioni relative ai conti bancari.

Tipologia di dati rubati: Dati di accesso degli utenti, password criptate, indirizzi email, date di nascita. Non sono state rubate le credenziali di carte di credito/debito.

Numeri: 50 milioni di dati rubati.

Costo stimato: Non dato.

Prevention paradigm: Sembra che le difese di LivingSocial non siano state efficaci in quanto non venivano utilizzati gli ultimi protocolli per la criptazione di dati. Nonostante

[26] LivingSocial http://en.wikipedia.org/wiki/LivingSocial

venisse usata una procedura di hash+salt per la criptazione dei dati, non venivano però utilizzate le versioni più recenti.

Response paradigm: Sono state avviate indagini attraverso enti privati e collaborazioni con la giustizia americana.

Technical: Nulla da rilevare.

Formal: Come abbiamo visto sopra, la società non utilizzava i più recenti metodi di criptazione e tantomeno si era adoperata nel creare un'infrastruttura che garantisse un alto livello di sicurezza. L'intrusione, si sarebbe potuto scongiurare se, oltre ad utilizzare degli algoritmi di criptazione più recenti, si fossero utilizzate metodologie come l'autenticazione a due fattori o un sistema di gestione delle chiavi come il FIPS 140-2[27].

Informal: Nulla da rilevare.

Caso dodici [48], [49]

Nome: Evernote Corporation.

Descrizione società[28]: Evernote è un'azienda indipendente privata con sede a Redwood City, California. E' stata fondata nel 2007 e i prodotti Evernote raggiungono più di 100 milioni di utenti nel mondo.

Descrizione fatto: Non è dato sapere molto sull'accaduto, tranne per il fatto che il sistema di sicurezza è riuscito a scovare attività sospette, le quali tentavano di accedere a dati protetti. Tramite un comunicato, l'azienda ha chiarito che nessun dato utente è stato rubato o modificato e che nessun dato di carte di credito/debito degli utenti premium è stato perso. Gli hacker sono però riusciti ad ottenere l'accesso ai database dove erano archiviate informazioni quali: username, password criptate e indirizzi email. Inoltre, la società ha rassicurato che le password erano criptate tramite l'utilizzo delle ultime tecnologie.

Quando: Marzo 2013

Cosa è stato colpito: Database societari.

Tipologia di dati rubati: Dati utenti come: username, password criptate, indirizzi email.

Numeri: 50 milioni di dati utente.

Costo stimato: Non dato

[27] FIPS 140-2 http://en.wikipedia.org/wiki/FIPS_140-2

[28] Evernote https://evernote.com/intl/it/corp/

Prevention paradigm: Evernote è una società che tiene in forte considerazione il tema della sicurezza, di qualsiasi informazione da lei archiviata. Lo dimostra il fatto che oltre ad essere in linea con tutti gli standard di sicurezza del settore, la società è sempre attiva, tramite campagne di sensibilizzazione e continui adattamenti, nello scongiurare qualsiasi tipo di attacco di questo genere.

Response paradigm: Appena venuti a conoscenza dell'intrusione, è stata inviata a tutti gli utenti un'email contenente un comunicato, il quale faceva chiarezza sull'accaduto e forniva delucidazioni riguardo cosa fosse stato rubato. La società ha inoltre allegato un elenco di best practice al fine di sensibilizzare i consumatori sulla tematica.

Technical: Dati non sufficienti.

Formal: Dati non sufficienti.

Informal: Dati non sufficienti.

Caso tredici [50], [51], [52], [53]

Nome: LinkedIn Corporation.

Descrizione società[29]: LinkedIn è un servizio web di rete sociale, gratuito (con servizi opzionali a pagamento), impiegato principalmente per lo sviluppo di contatti professionali. La rete di LinkedIn, presente in oltre 200 paesi, a gennaio 2009 contava circa 30 milioni di utenti, ha superato i 100 milioni di utenti il 22 marzo 2011 e i 200 milioni a gennaio 2013. Diffuso in tutti i continenti cresce a una velocità di 1 milione di iscritti a settimana.

Descrizione fatto: Il 5 giugno 2012, degli hacker russi sono riusciti ad ottenere l'accesso ai database societari riuscendo così ad entrare in possesso di password criptate per milioni di utenti. Qualche giorno dopo l'accaduto, le password comparvero in rete in chiaro (decriptate).

Quando: Giugno 2012

Cosa è stato colpito: Database societari.

Tipologia di dati rubati: Password criptate.

Numeri: 6.5 milioni di account rubati.

Costo stimato: Non dato.

[29] LinkedIn http://it.wikipedia.org/wiki/LinkedIn

Prevention paradigm: Nulla è dato su come gli hacker siano riusciti ad ottenere l'accesso ai server dove erano archiviati i dati ma, riguardo alla metodologia con la quale siano riusciti a decriptare un numero così elevato di password in un periodo relativamente breve, si pensa che sia causa del fatto che la società non abbia adottato le ultime tecnologie in campo criptografico. Dalle indagini effettuate infatti, emerge chiaramente che le password erano criptate senza l'utilizzo della procedura di salatura dell'algoritmo[30].

Response paradigm: Appena venuta a conoscenza dell'accaduto, la società ha immediatamente rilasciato una dichiarazione pubblica dove si affermava che, oltre alla partecipazione di diversi istituti di sicurezza informatica, si sarebbe denunciato l'accaduto all'FBI al fine di ottenere ulteriore supporto alle indagini. Successivamente, attraverso un secondo comunicato, la società dichiarava che non sarebbe stato possibile sapere se gli hacker fossero riusciti a rubare, oltre che le password, anche gli indirizzi email dei propri utenti. Fu pertanto impossibilitato l'accesso a quegli account che si pensa siano stati rubati.

Technical: Dati non sufficienti.

Formal: Come in altri casi visti finora, l'utilizzo di adeguate metodologie di criptazione, risulta essere un passaggio cruciale nel garantire la sicurezza dei dati archiviati. Sfortunatamente anche in questo caso tali misure di sicurezza necessitavano di un importante aggiornamento. Se si fosse utilizzata la procedura di "salatura" infatti, probabilmente gli hacker non sarebbero riusciti ad ottenere quel tipo di informazioni, evitando così l'emergere di ingenti costi legati al data breach.

Informal: Dati non sufficienti.

Caso quattordici [54], [55]

Nome: RockYou

Descrizione società[31]: Fondata nel 2005, RockYou è una società che si occupa dell'acquisizione dei diritti di videogiochi, applicarvi pubblicità in-game per poi rivendere tali titoli.

Descrizione fatto: Nel dicembre 2009, RockYou ha subito un ingente attacco, mirato all'ottenimento di informazioni quali username e password degli utenti. L'intrusione è

30 Sale (crittografia) http://it.wikipedia.org/wiki/Sale_(crittografia)

31 RockYou https://rockyou.com/about/

avvenuta tramite una SQL injection[32] con la quale gli hacker sono riusciti a penetrare all'interno del sistema dell'azienda e ad accedere ai database societari. In tali database, ogni informazione riservata era archiviata in chiaro. Nessuna cifratura era stata applicata né agli username né tantomeno alle password, agevolando così di molto il lavoro degli hacker.

Quando: Dicembre 2009

Cosa è stato colpito: Sistema e database societari.

Tipologia di dati rubati: Username e password.

Numeri: 32 milioni di account rubati.

Costo stimato: Non dato.

Prevention paradigm: La società era in possesso di un pessimo livello di sicurezza. I dati erano memorizzati in chiaro ed erano facilmente accessibili da qualsiasi postazione, una volta ottenuto l'accesso al network. Vi erano inoltre altre inefficienze ricollegabili alle comuni prassi di sicurezza nella gestione degli account.

Response paradigm: Anche l'incidente era stato affrontato in maniera pessima. Anzitutto, i clienti non erano stati avvisato in alcun modo dell'accaduto se non 10 giorni dopo l'incidente. Questo comportamento ha esposto la clientela ad ulteriori danni, ad esempio per il fatto che la maggior parte degli utenti utilizzi le medesime credenziali d'accesso in ogni sito web, ha negato loro la possibilità di disporre di misure preventive contro possibili intrusioni in network differenti. Altro comportamento inappropriato, è stato quello di non cessare il servizio una volta venuti a conoscenza dell'accaduto. Questo ha fatto sì che hacker siano stati agevolati nel disporre a proprio piacimento dei dati acquisiti.

Technical: Chiara esposizione ad attacchi tramite SQL injection.

Formal: Adozione di pessime policy di sicurezza interne. Memorizzazione di dati non criptati e facile accesso ad ogni layer del network.

Informal: Nulla da rilevare.

[32] SQL injection http://it.wikipedia.org/wiki/SQL_injection

Caso quindici [56], [57]

Nome: Cupid Media Ltd.

Descrizione società[33]: Cupid Media è una società che gestisce siti d'incontri. La piattaforma è disponibile in diverse lingue sin dalla sua fondazione nel 2000. La sua sede si trova sulla Gold Cast nel Queensland, Australia.

Descrizione fatto: Nel gennaio 2013, alcuni hacker, sfruttando delle vulnerabilità della piattaforma server ColdFusion di Adobe, sono riusciti a penetrare all'interno dei database di Cupid Media. Gli hacker sono stati abili nel caricare all'interno della piattaforma un file capace di eseguire una serie ripetuta di query SQL (SQL injection) riuscendo così ad ottenere l'accesso ai database della società. Una volta dentro, gli hacker sono entrati in possesso di numerose informazioni come nominativi, indirizzi email, password, date di nascita. Anche in questo caso, tutti i dati erano archiviati in chiaro. La natura del servizio forniva inoltre molte informazioni aggiuntive riferibili ai fruitori del servizio, come ad esempio: preferenze sessuali, religione, etnia.

Quando: Inizio 2013

Cosa è stato colpito: Piattaforma server e database aziendali.

Tipologia di dati rubati: Nominativi, indirizzi email, password non criptate e date di nascita dei clienti.

Numeri: Oltre 42 milioni di dati utente.

Costo stimato: Non dato.

Prevention paradigm: Diverse sono state le cause dell'incidente. Una è riferibile a delle debolezze della piattaforma server nei confronti degli attacchi SQL injection. Ancora, la mancata criptazione dei dati archiviati. Questo dovrebbe essere una fase basilare nella messa in sicurezza dei dati ma, a quanto pare non vi era stata attribuita la dovuta importanza o si era fatto un eccessivo affidamento ad altri tipi di sicurezza.

Response paradigm: Dopo l'incidente sono state avviate le indagini tramite delle società specializzate ed immediatamente si è tentato di rimediare al danno adottando la criptazione dei dati.

Technical: La piattaforma server utilizzata, presentava bug di programmazione e gli hacker sono stati abili nello sfruttarla tramite un'operazione di SQL injection. Dopo l'accaduto è

33 Cupid Media http://en.wikipedia.org/wiki/Cupid_Media

stata anche contattata la Adobe per ulteriori chiarimenti sui motivi per la quale tale bug non fosse stato scovato prima.

Formal: Il livello delle policy interne può ritenersi estremamente basso, dal momento che non era stato adottato alcun tipo di criptazione dei dati archiviati. Data la rilevanza dei dati in possesso, la società avrebbe dovuto redigere un sistema di sicurezza capace di garantire la confidenzialità di qualsiasi informazione inerente alle proprie attività. Probabilmente si era fatto un eccessivo affidamento ai sistemi di sicurezza delle reti o ancora, non era ben chiara la rilevanza di tali dati in loro possesso.

Informal: Nulla da rilevare.

Caso sedici [58], [59], [60]

Nome: RSA Security Inc.

Descrizione società[34]: RSA Security è una società per azioni specializzata in sicurezza informatica. Il suo quartier generale si trova a Bedford nel Massachusetts, ma mantiene degli uffici in Irlanda, nel Regno Unito, a Singapore e in Giappone. La compagnia che attualmente è nota come RSA Security inizialmente era conosciuta come Security Dynamics finché la RSA Data Security non la acquisì nel giugno del 1996. Nel 1997 la società acquisì anche la DynaSoft AB e nel febbraio 2001 acquisì la Xcert International, Inc una compagnia privata che sviluppava sistemi basati su certificati digitali per l'e-commerce. Nel maggio del 2001 acquisì la 3-G International, Inc una compagnia privata ad alta innovazione che sviluppava smart card e sistemi di autentificazione biometrici. Nell'agosto 2001 venne acquisita la Securant Technologies, Inc, una compagnia privata che sviluppava ClearTrust, un sistema di gestione dell'identità digitale.

Descrizione fatto: Il 17 marzo 2011, RSA annuncia di aver subito subito un attacco informatico ai propri sistemi, specificatamente sui prodotti two-factor autentication key. La società non ha rilasciato ulteriori informazioni in quanto sostiene che queste potrebbero ridurre l'efficacia del funzionamento dei propri prodotti.

Quando: Marzo 2011

Cosa è stato colpito: Sistema di funzionamento dei prodotti two-factor autentication e computer dei dipendenti.

Tipologia di dati rubati: Non dato.

[34] RSA Security http://it.wikipedia.org/wiki/RSA_Security

Numeri: Non dato.

Costo stimato: Più di 66 milioni di dollari.

Prevention paradigm: Si riesce a far luce sul caso solamente qualche mese dopo l'accaduto. Durante le indagini, emerge che l'attacco era partito da un virus installato sul computer di un dipendente di RSA, il quale ingenuamente era caduto vittima di un attacco di phishing email. Tale virus, una volta avviato tramite l'email infetta, era stato in grado di fruttare un bug proprio di adobe flash player, con la quale poi si è stati in grado di entrare in possesso della macchina, ottenendo così l'accesso anche al sistema di RSA.

Response paradigm: Date le mancate dichiarazioni ufficiali sull'accaduto, l'impatto della violazione sui clienti rimane tutt'ora sconosciuto. Nel tentativo di rimediare al danno e, per tentare di arginare il potere degli hacker, la società ha dato la possibilità ai propri clienti di entrare in possesso di nuovi token, naturalmente in modo completamente gratuito.

Technical: Nulla da rilevare.

Formal: Nulla da rilevare.

Informal: Dalle indagini condotte, sembra che la causa dell'incidente sia stata un'email infetta indirizzata ad un dipendente di RSA. Questa, conteneva un particolare virus capace di sfruttare un bug in Adobe Flash Player e di creare così una backdoor con la quale gli hacker sarebbero stati in grado di gestire da remoto il computer.

Caso diciassette [12], [61], [62], [63]

Nome: SK Communications.

Descrizione società[35]: SK Communications è una società Sud Coreana, la quale si occupa di fornire servizi di server provider. Il suo prodotto più famoso è Nate, il quale nel 2003 si è fuso con CyWorld che è uno dei più famosi social network del paese.

Descrizione fatto: Il 28 luglio 2011, SK Communications annuncia di esser stata vittima di un attacco informatico il quale ha sottratto 35 milioni di dati personali riferibili ai propri utenti. I dati compromessi erano degli utenti di CyWorld (il più grande social network del Sud Corea) e di Nate (popolare portale web sudcoreano). Tra il 18 e il 25 luglio 2011, gli hacker hanno infettato più di 60 pc della società, riuscendo così ad ottenere l'accesso ai database dove vi erano archiviati i dati utente. Gli hacker, per riuscire nel loro intento e così, riuscire ad

35 SK Communications http://en.wikipedia.org/wiki/SK_Communications

installare il malware sulle macchine di SK, dapprima compromisero i server di una società terza, la quale era fornitrice di vari servizi, tra cui anche della gestione del sistema informatico. Una volta riusciti a manipolare questi server, gli hacker sostituirono delle pach d'aggiornamento con un trojan, il quale ebbe facile accesso ai computer di SK Communications.

Quando: Luglio 2011

Cosa è stato colpito: Server di terze parti, computer e database societari.

Tipologia di dati rubati: Nomi, numeri telefonici, indirizzi email e di residenza, date di nascita, password, dettagli di genere, identificatori d'utenti (solamente le password e i numeri di registrazione erano criptati).

Numeri: 35 milioni di persone. E' considerato il più grande furto di informazioni personali della storia nel Sud Corea e dal momento che questa conta circa 49 milioni di persone, può dirsi che più della metà della popolazione è stata colpita.

Costo stimato: Non dato

Prevention paradigm: Gli hacker sono riusciti a bypassare molteplici antivirus e sistemi di sicurezza senza essere notati e fermati in alcun modo. Tale evento sottolinea appunto l'imprevedibilità di attacchi di questo genere e quindi di quanto sia difficile instaurare misure preventive che rendano vani tali rischi. SK, avendo adottato ogni misura necessaria a garantire un forte margine di sicurezza, non poteva prevedere un'azione di questo genere. Proprio per tale motivo, ribadiamo ancora una volta che una società operante in un ambiente simile, debba necessariamente concentrarsi più sulla risposta che sulla prevenzione.

Response paradigm: In risposta all'accaduto, la società ha imposto la rimozione di ogni programma marchiato EST Soft, società responsabile dell'installazione e della manutenzione dell'intero sistema di sicurezza (il quale è stato ritenuto responsabile di non essere stato in grado di scovare il malware prima che questo fosse messo in funzione). Sono inoltre state aggiornate le procedure di sicurezza, in modo da far sì che un simile evento non possa più accadere in futuro. La società si è inoltre presentata in giudizio per risarcire i danni ai consumatori danneggiati.

Technical: Sul fronte tecnico, si sarebbero potuti adottare ulteriori software capaci di individuare programmi fraudolenti (come l' Host-Based Intrusion Prevent System, HIPS, visto in precedenza nel caso di JP Morgan) o, in alternativa misure preventive come una più dettagliata scansione preventiva dei programmi scaricati.

Formal: Sul lato formale, si sarebbero potute adottare politiche di sicurezza qualitativamente migliori nel momento in cui avveniva lo scambio di informazioni con società terze (anche nel caso in cui si trattassero di fornitori verificati), proprio come si sarebbe dovuto fare nel caso Target.

Informal: Nulla da rilevare.

Caso diciotto [64], [65]

Nome: Premera Blue Cross

Descrizione società[36]: Premera è un'associazione no profit che si occupa di fornire assicurazioni sanitarie. La sua sede principale è in Mountlake Terrace, Washington.

Descrizione fatto: Nonostante l'incidente si sia verificato nel maggio 2014, la società ne è venuta a conoscenza solamente nel gennaio 2015. L'attacco ha coinvolto sia Premera Blue Cross che Premera Blue Cross Blue Shield d'Alaska e ha coinvolto un gran numero di clienti, i quali dati rubati sono riferibili ad informazioni finanziarie, mediche, date di nascita e social security numbers. Premera ha inoltre fatto sapere che i dati non sono stati rimossi dai propri database e che non vi sono evidenze di un loro uso inappropriato. Informazioni sulla dinamica dell'incidente non sono disponibili ma, si pensa che a condurre l'attacco sia stato un gruppo di hacker cinese (si pensa addirittura che questi possano essere stati supportati dal governo).

Quando: Gennaio 2015.

Cosa è stato colpito: Database societari.

Tipologia di dati rubati: Dati medici, finanziari e personali.

Numeri: Dati per 11 milioni di clienti.

Costo stimato: Non dato.

Prevention paradigm: Non dato.

Response paradigm: Premera ha dichiarato di aver contattato personalmente, tramite posta, tutti quei clienti i cui dati sono stati sottratti durante l'incidente. Si è inoltre impegnata di offrire loro due anni di servizi gratuiti come risarcimento. La società ha inoltre fatto sapere che sta collaborando con la società Mandiant e con l'FBI per investigare sul caso.

Technical: Non dato.

Formal: Non dato.

---

[36] Premera Blue Cross http://en.wikipedia.org/wiki/Premera_Blue_Cross

Informal: Non dato.

Caso diciannove [66], [67], [68]

Nome: VeriSign Inc.

Descrizione società[37]: VeriSign, Inc. è una società statunitense con sede a Reston, in Virginia, che gestisce un'ampia gamma di infrastrutture di Rete, fra cui due dei tredici server dei nomi radice operanti in Internet, il registro con autorità per i Domini di primo livello generici .com, .net e .name, nonché per i domini di primo livello con codice paese .cc e .tv e i sistemi di back-end per i domini di primo livello .jobs e .edu. Verisign offre inoltre tutta una serie di servizi di sicurezza, quali managed DNS, Distributed Denial of Service (DDoS) e reporting di minaccia informatica. Nel 2010 Verisign ha ceduto la propria attività di autenticazione – comprendente i servizi Secure Sockets Layer (SSL), PKI (public key infrastructure), Verisign Trust Seal e Verisign Identity Protection (VIP) – a Symantec per 1,28 miliardi di dollari.

Descrizione fatto: Nel 2010, Verisign è stata oggetto di numerosi attacchi informatici ma il top management ne è venuto a conoscenza solamente nel settembre 2011. Attraverso un attacco al network della compagnia, gli hacker hanno ottenuto l'accesso ad un ristretto numero di computer e server della società. Si pensa che questi, possano aver utilizzato il servizio di DNS di Verisign per indirizzare i naviganti verso determinati siti web così da infettare i propri computer. Il tutto però non è stato confermato dalla società che, nonostante le numerose indagini nega che l'integrità del sistema DNS sia stata compromessa.

Quando: 2010

Cosa è stato colpito: Network societario, computers e servers

Tipologia di dati rubati: Non dato.

Numeri: Non dato.

Costo stimato: Non dato.

Prevention paradigm: Tutte le zone DNS erano protette da una serie di controlli d'integrità, incluso un monitoraggio e una validazione in tempo reale. Verisign afferma di porre sempre la massima attenzione in tema di sicurezza, specialmente nei servizi di DNS

[37] Verisign http://it.wikipedia.org/wiki/Verisign

Response paradigm: La società ha ammesso di essere ignara riguardo la dinamica dell'accaduto. E' stato dichiarato che, data la natura dell'attacco, non si può assicurare che gli interventi attuati in risposta all'attacco possano essere sufficienti a garantire la protezione da un nuovo incidente di questo genere. La risposta all'attacco è stata immediata ma, i tecnici non hanno informato tempestivamente il top management riguardo l'accaduto e ciò ha fatto sì che venissero alla luce ulteriori problematiche di comunicazione interna.

Technical: Non dato.

Formal: Non dato.

Informal: Non dato.

Caso venti [69], [70]

Nome: AOL Inc.

Descrizione società[38]: AOL Inc. è una multinazionale mass media, nel 2006, era il più grande internet service provider del mondo con i suoi 30 milioni di utenti.

Descrizione fatto: Nell'aprile 2014, AOL dichiara di aver subito un attacco diretto al proprio network e ai propri sistemi. La dichiarazione dell'intrusione è pressoché contestuale e, viene specificato, con un post sul proprio blog, che ogni mezzo sarà utilizzato nel tentativo di far luce sull'accaduto. A seguito dell'incidente, attraverso le dovute indagini, si chiarisce che oggetto dell'attacco siano state le email della clientela. E' stato inoltre chiarito che non sono stati sottratti alcun tipo di dati finanziari.

Quando: Aprile 2014.

Cosa è stato colpito: Network, sistema e server aziendali.

Tipologia di dati rubati: Email degli utenti, indirizzi postali, informazioni personali come il numero di telefono, password criptate, domande di sicurezza criptate, alcune informazioni riguardante i dipendenti.

Numeri: Circa il 2% degli account AOL.

Costo stimato: Non dato.

Prevention paradigm: La metodologia di criptazione utilizzata per proteggere le password, le domande di sicurezza e i dati finanziari sembra aver avuto successo in quanto,

[38] AOL http://it.wikipedia.org/wiki/AOL

come ha dichiarato la stessa AOL, sembrerebbe che gli hacker non siano riusciti ad usufruire di tali informazioni.

Response paradigm: In risposta all'attacco, la società si è immediatamente attivata nelle indagini con l'ausilio di importanti firme del settore e con il supporto delle autorità giudiziarie. Sono state inoltre inviate email di notifica ai possibili utenti bersaglio dell'attacco.

Technical: Non dato.

Formal: Non dato.

Informal: Non dato.

Caso ventuno. [71], [72]

Nome: Monster Worldwide Inc.

Descrizione società[39]: Monster.com è uno dei siti per cercare lavoro più visitati al mondo. Appartenente alla Monster Worldwide Inc., è stato creato nel 1999 dalla fusione di The Monster Board (TMB) e Online Career Center (OCC) che già erano tra i più famosi siti per cercare lavoro. Monster.com indirizza i lavoratori in cerca d'occupazione verso posti di lavoro le quali richieste combaciano con le proprie skill.

Descrizione fatto: La società, nella metà del 2007 ha subito un attacco, diretto alle proprie strutture informatiche il quale ha reso disponibile agli hacker un ingente numero di informazioni. Non è dato sapere molto sulla dinamica dell'incidente ma, la società ha dichiarato che probabilmente è stata attaccata più di una volta e che comunque il sistema di sicurezza in se non è stato intaccato dal momento che gli hacker avrebbero guadagnato l'accesso al sistema tramite chiavi legittime.

Quando: Luglio 2007

Cosa è stato colpito: Database societari.

Tipologia di dati rubati: Si pensa solamente gli indirizzi email dei clienti.

Numeri: Dati riguardanti 1.3 milioni di persone

Costo stimato: Non dato.

Prevention paradigm: Monster.com si è difesa affermando che il proprio sistema di sicurezza non sia stato violato. Gli hacker sarebbero riusciti ad ottenere delle chiavi d'accesso

[39] Monster.com http://en.wikipedia.org/wiki/Monster.com

totalmente legittime, ottenendo così il completo accesso al sistema. Probabilmente sono entrati in possesso di tali chiavi tramite attività di phishing o tramite una libreria di dati rubati in seguito ad un precedente data breach

Response paradigm: La risposta della società è stata alquanto vaga, in quanto ha solamente affermato di essere disposta a spendere fino ad 80 milioni di dollari per effettuare l'update del sito e renderlo così più sicuro.

Technical: Non dato.

Formal: Non dato.

Informal: Non dato.

Caso ventidue. [73], [74]

Nome: Experian plc.

Descrizione società[40]: Experian è un gruppo globale che fornisce servizi d'informazione ed opera in 40 stati. Il gruppo ha sede in Dublino ma ha sedi primarie sparse per il mondo. E' quotata al London Stock Exchange. Nel 1996, quando andava sotto il nome di TRW Information Services, era stata acquistata da GUS plc ma, nel 2006 è uscita dal gruppo GUS rendendosi così, totalmente indipendente e potersi quotare sulla borsa londinese. Con il nome TRW, la società era un ufficio di credito, il quale, utilizzando la linea telefonica, trasmetteva informazioni come: storie di credito, documenti di lavoro, fallimenti, insolvenze sui prestiti e il codice fiscale dei propri clienti.

Descrizione fatto: TRW era stata violata dopo che degli hacker erano riusciti ad entrare in possesso di una password segreta e di un manuale sul funzionamento del sistema. La password era stata persa nel 1983 ma, nulla fu detto da parte di TRW fino al 1984. Gli hacker sono riusciti a raggiungere i database dove erano archiviati dati confidenziali sugli utenti ma, riuscirono solo a leggerli, senza poterli modificare. Questo può dirsi come il primo vero data breach della storia capace di mettere in pericolo le informazioni personali di milioni di utenti.

Quando: Luglio 1984

Cosa è stato colpito: Database societari.

Tipologia di dati rubati: Dati di carte di credito.

Numeri: Informazioni su 90 milioni di clienti furono rubate.

---

40 Experian http://en.wikipedia.org/wiki/Experian

Costo stimato: Non dato.

Prevention paradigm: Il sistema di sicurezza adottato da TRW era molto semplice da eludere. Per l'identificazione dell'utente, questo si serviva di due codici: uno a 7 cifre per identificare l'utente e uno più corto utilizzato come password segreta. Il primo era relativamente poco protetto e altrettanto semplice da ottenere mentre per il secondo, non essendo il sistema di autenticazione estremamente potente, era facilmente ottenibile tramite delle forzature al sistema.

Response paradigm: Non dato.

Technical: Non dato.

Formal: Non dato.

Informal: Non dato.

Caso ventitré [75], [76]

Nome: Yahoo! Inc.

Descrizione società[41]: Yahoo! è una società fornitrice di servizi internet rivolta al mondo business e consumer, fondata nel 1994 da David Filo e Jerry Yang, allora studenti presso la Stanford University. Conosciuta principalmente per la sua funzione di motore di ricerca, si compone anche di moltissimi altri servizi rivolti alla comunicazione (mail, messenger e chat) e grazie a partnership si propone anche nel mercato dei media. La maggioranza dei suoi servizi sono offerti in 20 lingue e la sua struttura è localizzata per 25 nazioni.

Descrizione fatto: Nel maggio 2013, Yahoo comunica di aver subito un attacco informatico dove circa 22 milioni di username sono stati rubati. Gli hacker sono riusciti ad entrare in possesso solamente degli username, senza riuscire a scovare le password o qualsiasi altro dato.

Quando: Maggio 2013.

Cosa è stato colpito: Network aziendale.

Tipologia di dati rubati: Username.

Numeri: 22 milioni di username (10% degli utenti di Yahoo! Japan).

Costo stimato: Non dato.

Prevention paradigm: Non dato.

41 Yahoo! http://it.wikipedia.org/wiki/Yahoo!

Response paradigm: Come risposta all'attacco, dal momento che il sistema di sicurezza era riuscito ad identificare l'intrusione quando questa non era ancora terminata, i tecnici di Yahoo! hanno prontamente tagliato ogni collegamento con la rete esterna proprio al fine di evitare ulteriori fuoriuscite di dati. Successivamente all'incidente, Yahoo! Japan ha comunicato immediatamente l'accaduto al pubblico tramite un post sul proprio blog. Inoltre, in via precauzionale la società ha raccomandato i propri utenti di modificare le proprie password.

Technical: La violazione del sistema di Yahoo è stata effettuata tramite una SQL injection, alla quale però la società ha prontamente risposto effettuando un aggiornamento del sistema.

Formal: Non dato.

Informal: Non dato.

Bibliografia

[1] R. Baskerville, P. Spagnoletti, J. Kim, Incident-centered information security: Managing a strategic balance between prention and response. Information & Management 51 (2014), pp. 138-151

[2] Åhlfeldt R.M., Spagnoletti P. and Sindre G. (2007), Improving the Information Security Model by using TFI. In "New Approaches for Security, Privacy and Trust in Complex Environments", IFIP Springer Series, Springer Boston, Volume 232/2007, 73-84

[3] O. Hanseth, C. Ciborra (2007), Risk, Complexity and ICT. Edward Elgar; Chaltenham, UK – Northampton, MA, USA, pp. 75-90

[4] W. Xu, G. Grant, H. Nguyen, X. Dai (2008), Security Breach: The Case of TJX Companies, Inc. Communications of the Association for Information Systems,Volume 23 Article 31

[5] T. Radichel (2014), Case Study: Critical Controls that Could Have Prevented Target Breach. SANS Institute InfoSec Reading Room.

[6] J. S. Cheney (2010), Heartland Payment Systems: Lessons Learned from a Data Breach. Payment Cards Center, Federal Reserve Bank of Philadelphia.

[7] A. Jeng (2015), Minimizing Damage From J.P. Morgan's Data Breach. SANS Institute InfoSec Reading Room.

[8] Stoppage of Play: The Sony PlayStation Network Crash (A).

[9] Sombers Associates, Inc., and W. H. Highleyman (2014), eBay's Slow Response to Data Hack. The Availability Digest.

[10] The British Standards Institution (2014), LESSONS LEARNED: Home Depot Security Breach. The British Standards Institution.

[11] The Home Depot (2014), The Home Depot Reports Findings in Payment Data Breach Investigation. The Home Depot.

[12] Command Five Pty Ltd (2011), SK Hack by an Advanced Persistent Threat. Command Five Pty Ltd.

[13] Risk Based Security, Inc. (2014), Data Breach QuickView An Executive's Guide to 2013 Data Breach Trends. Risk Based Security, Inc.

[14] PCI Security Standards Council, PCI DSS Requirements and Security Assessment Procedures, Version 2.0, ottenuto nel maggio 2015 da https://www.pcisecuritystandards.org/documents/pci_dss_v2.pdf

[15] Ponemon Institute (2012), 2011 Cost of Data Breach Study: United States, Benchmark Research sponsored by Symantec Independently Conducted by Ponemon Institute LLC, Ponemon Institute.

[16] Perrow, C. ([1984]1999), Normal Accidents: Living With High-Risk Technologies, New Jersey, USA: Princeton University Press.

[17] La Porte, T.R. (1988), 'The United States air traffic system: increasing reliability in the midst of rapid growth', in Renate Mayntz and Thomas P. Hughes (eds), The Development of Large Technical Systems, Boulder, CO: Westview Press, pp. 215–44

[18] Levinthal, D.A. and J.G. March (1993), 'The myopia of learning', Strategic Management Journal, 14, 95–112.

[19] P. Stephenson, Managing digital incidents – a background, Computer Fraud & Security 2004 (12), 2004, pp. 17–19.

Sitografia

[20] P. Duckling (2013), Anatomy of a password disaster - Adobe's giant-sized cryptographic blunder [online]. Disponibile al seguente indirizzo: https://nakedsecurity.sophos.com/2013/11/04/anatomy-of-a-password-disaster-adobes-giant-sized-cryptographic-blunder [Visualizzato il 29 maggio 2015]

[21] B. Krebs (2013), Adobe Breach Impacted At Least 38 Million Users [online]. Disponibile al seguente indirizzo: http://krebsonsecurity.com/2013/10/adobe-breach-impacted-at-least-38-million-users/#more-23030 [Visualizzato il 29 maggio 2015]

[22] P. Duckling (2013), Adobe customer data breached - login and credit card data probably stolen, all passwords reset [online]. Disponibile al seguente indirizzo: https://nakedsecurity.sophos.com/2013/10/04/adobe-owns-up-to-getting-pwned-login-and-credit-card-data-probably-stolen-all-passwords-reset [Visualizzato il 29 maggio 2015]

[23] D. Rampe (2013) Bad to Worse. Update: 38 Milion Adobe Users Could Be at Risk of ID Theft in Recent Breach. Photoshop Source Code Also Compromised [online]. http://www.threatmetrix.com/bad-to-worse-update-38-million-adobe-users-could-be-at-risk-of-id-theft-in-recent-breach-photoshop-source-code-also-compromised/ [Visualizzato il 29 maggio 2015]

[24] J. Pepitone (2014), 5 of the biggest-ever credit card hacks [online]. Disponibile al seguente indirizzo: http://money.cnn.com/gallery/technology/security/2013/12/19/biggest-credit-card-hacks/index.html [Visualizzato il 29 maggio 2015]

[25] C. Marciano (2013), Target Data Breach Insurance Case Study [online]. Disponibile al seguente indirizzo: http://databreachinsurancequote.com/data-breach-case-study/target-data-breach-insurance-case-study/ [Visualizzato il 30 maggio 2015]

[26] R. King (2009), Lessons from the Data Breach at Heartland [online]. Disponibile al seguente indirizzo: http://www.bloomberg.com/bw/stories/2009-07-06/lessons-from-the-data-breach-at-heartlandbusinessweek-business-news-stock-market-and-financial-advice [Visualizzato il 30 maggio 2015]

[27] S. Hays (2012), A Famous Data Security Breach & PCI Case Study: Four Years Later [online]. Disponibile al seguente indirizzo: http://www.secureworks.com/resources/blog/general-pci-compliance-data-security-case-study-heartland/#sthash.VtyfVvpC.dpuf [Visualizzato il 30 maggio 2015]

[28] B. Fulks (2011), The PlayStation Network Attack [online]. Disponibile al seguente indirizzo: http://www.brighthub.com/computing/smb-security/articles/123382.aspx [Visualizzato il 3 giugno 2015]

[29] Veracode, Sony PSN Breach Infographic [online]. Disponibile al seguente indirizzo: http://www.veracode.com/sony-psn-breach-infographic [Visualizzato il 3 giugno 2015]

[30] Venturebeat (2011), Security lessons from the PlayStation Network breach [online]. Disponibile al seguente indirizzo: http://venturebeat.com/2011/09/22/security-lessons-from-the-playstation-network-breach/ [Visualizzato il 3 giugno 2015]

[31] F. Y. Rashid (2011), Epsilon Data Breach to Cost Billions in Worst-Case Scenario [online]. Disponibile al seguente indirizzo: http://www.eweek.com/c/a/Security/Epsilon-Data-Breach-to-Cost-Billions-in-WorstCase-Scenario-459480 [Visualizzato il 3 giugno 2015]

[32] T. Bradley (2011), Epsilon Data Breach: Expect a Surge in Spear Phishing Attacks [online]. Disponibile al seguente indirizzo: http://www.pcworld.com/article/224192/epsilon_data_breach_expect_a_surge_in_spear_phishing_attacks.html [Visualizzato il 3 giugno 2015]

[33] K. Dearne (2011), Epsilon email security breach widens [online]. Disponibile al seguente indirizzo: http://www.theaustralian.com.au/business/technology/epsilon-email-security-breach-widens/story-e6frgakx-1226035279855 [Visualizzato il 3 giugno 2015]

[34] M. J. Schwartz (2011), Epsilon Fell To Spear-Phishing Attack [online]. Disponibile al seguente indirizzo: http://www.darkreading.com/attacks-and-breaches/epsilon-fell-to-spear-phishing-attack/d/d-id/1097119? [Visualizzato il 3 giugno 2015]

[35] M. Lennon (2011), Massive Breach at Epsilon Compromises Customer Lists of Major Brands [online]. Disponibile al seguente indirizzo: http://www.securityweek.com/massive-breach-epsilon-compromises-customer-lists-major-brands [Visualizzato il 3 giugno 2015]

[36] B. Sullivan (2005), 40 million credit card exposed [online]. Disponibile al seguente indirizzo: http://www.nbcnews.com/id/8260050/ns/technology_and_science-security/t/million-credit-cards-exposed/#.VXCik2BSW8q [Visualizzato il 3 giugno 2015]

[37] A. Litan (2005), CardSystems Flaw Shows Deep Credit-Card Security Problems [online]. Disponibile al seguente indirizzo: https://www.gartner.com/doc/484499/cardsystems-flaw-shows-deep-creditcard [Visualizzato il 3 giugno 2015]

[38] J. Evers (2005), Credit card breach exposes 40 million accounts [online]. Disponibile al seguente indirizzo: http://news.cnet.com/Credit-card-breach-exposes-40-million-accounts/2100-1029_3-5751886.html [Visualizzato il 3 giugno 2015]

[39] B. Schneier (2005), CardSystems Exposes 40 Million Identities [online]. Disponibile al seguente indirizzo: https://www.schneier.com/blog/archives/2005/06/cardsystems_exp.html [Visualizzato il 3 giugno 2015]

[40] S. Tobias (2014), 2014: The Year in Cyberattacks [online]. Disponibile al seguente indirizzo: http://www.newsweek.com/2014-year-cyber-attacks-295876 [Visualizzato il 3 giugno 2015]

[41] M. Goldstein (2014), Neglected Server Provided Entry for JPMorgan Hackers [online]. Disponibile al seguente indirizzo: http://dealbook.nytimes.com/2014/12/22/entry-point-of-jpmorgan-data-breach-is-identified/?ref=technology&_r=0 [Visualizzato il 3 giugno 2015]

[42] G. Kelly (2014), eBay Suffers Massive Security Breach, All Users Must Change Their Passwords [online]. Disponibile al seguente indirizzo: http://www.forbes.com/sites/gordonkelly/2014/05/21/ebay-suffers-massive-security-breach-all-users-must-their-change-passwords/ [Visualizzato il 3 giugno 2015]

[43] B. Krebs (2014), Home Depot: Hackers Stole 53M Email Addresses [online]. Disponibile al seguente indirizzo: http://krebsonsecurity.com/2014/11/home-depot-hackers-stole-53m-email-addreses/ [Visualizzato il 9 giugno 2015]

[44] B. Krebs (2014), Banks: Credit Card Breach at Home Depot [online]. Disponibile al seguente indirizzo: http://krebsonsecurity.com/2014/09/banks-credit-card-breach-at-home-depot/ [Visualizzato il 9 giugno 2015]

[45] Livingsocial, LivingSocial security notice [online]. Disponibile al seguente indirizzo: https://www.livingsocial.com/createpassword [Visualizzato il 9 giugno 2015]

[46] N. Perlroth (2013), LivingSocial Hack Exposes Data for 50 Million Customers [online]. Disponibile al seguente indirizzo: http://bits.blogs.nytimes.com/2013/04/26/living-social-hack-exposes-data-for-50-million-customers/ [Visualizzato il 9 giugno 2015]

[47] L. Townsend (2013), How LivingSocial Could Have Avoided a Data Breach [online]. Disponibile al seguente indirizzo: http://web.townsendsecurity.com/bid/64685/How-LivingSocial-Could-Have-Avoided-a-Data-Breach [Visualizzato il 9 giugno 2015]

[48] T. Mogg (2013), Evernote hack: 50 million users forced to reset passwords [online]. Disponibile al seguente indirizzo: http://www.digitaltrends.com/mobile/evernote-hack-50-million-users-forced-to-reset-passwords/ [Visualizzato il 9 giugno 2015]

[49] D. Engberg (2013), Security Notice: Service-wide Password Reset [online]. Disponibile al seguente indirizzo: https://blog.evernote.com/blog/2013/03/02/security-notice-service-wide-password-reset/ [Visualizzato il 9 giugno 2015]

[50] I. Paul (2012), Update: LinkedIn Confirms Account Passwords Hacked [online]. Disponibile al seguente indirizzo: http://www.pcworld.com/article/257045/6_5m_linkedin_passwords_posted_online_after_apparent_hack.html [Visualizzato il 9 giugno 2015]

[51] J. Finkle, J. Saba (2012), LinkedIn suffers data breach - security experts [online]. Disponibile al seguente indirizzo: http://in.reuters.com/article/2012/06/06/linkedin-breach-idINDEE8550EN20120606 [Visualizzato il 9 giugno 2015]

[52] Wikipedia, 2012 LinkedIn hack [online]. Disponibile al seguente indirizzo: http://en.wikipedia.org/wiki/2012_LinkedIn_hack [Visualizzato il 9 giugno 2015]

[53] C. Velazco, (2012) 6.5 Million LinkedIn Passwords Reportedly Leaked, LinkedIn Is "Looking Into" It [online]. Disponibile al seguente indirizzo: http://techcrunch.com/2012/06/06/6-5-million-linkedin-passwords-reportedly-leaked-linkedin-is-looking-into-it/ [Visualizzato il 9 giugno 2015]

[54] N. Cubrilovic (2009), RockYou Hack: From Bad To Worse [online]. Disponibile al seguente indirizzo: http://techcrunch.com/2009/12/14/rockyou-hack-security-myspace-facebook-passwords/ [Visualizzato il 9 giugno 2015]

[55] J. Vijayan (2009), RockYou hack exposes names, passwords of 30M accounts [online]. Disponibile al seguente indirizzo: http://www.computerworld.com/article/2522045/security0/rockyou-hack-exposes-names--passwords-of-30m-accounts.html [Visualizzato il 9 giugno 2015]

[56] B. Krebs (2013), Cupid Media Hack Exposed 42M Passwords [online]. Disponibile al seguente indirizzo: http://krebsonsecurity.com/2013/11/cupid-media-hack-exposed-42m-passwords/ [Visualizzato il 9 giugno 2015]

[57] P. Cowan (2014), Cupid Media found culpable for password data breach [online]. Disponibile al seguente indirizzo: http://www.itnews.com.au/News/388823,cupid-media-found-culpable-for-password-data-breach.aspx [Visualizzato il 9 giugno 2015]

[58] M. J. Schwartz (2011), RSA SecurID Breach Cost $66 Million [online]. Disponibile al seguente indirizzo: http://www.darkreading.com/attacks-and-breaches/rsa-securid-breach-cost-$66-million/d/d-id/1099232? [Visualizzato il 9 giugno 2015]

[59] J. Jarmoc (2011), RSA compromise: Impacts on SecurID [online]. Disponibile al seguente indirizzo: http://www.secureworks.com/cyber-threat-intelligence/threats/rsacompromise/ [Visualizzato il 9 giugno 2015]

[60] A. Moscaritolo (2011) Researchers study actual file used in RSA SecurID breach [online]. Disponibile al seguente indirizzo: http://www.scmagazine.com/researchers-study-actual-file-used-in-rsa-securid-breach/article/210612/ [Visualizzato il 9 giugno 2015]

[61] D. Goodin (2011), Software maker fingered in Korean hackocalypse [online]. Disponibile al seguente indirizzo: http://www.theregister.co.uk/2011/08/12/estsoft_korean_megahack/ [Visualizzato il 9 giugno 2015]

[62] L. Tung (2011), Anatomy of a cunning APT: the SK Communications breach [online]. Disponibile al seguente indirizzo: http://www.cso.com.au/article/402450/anatomy_cunning_apt_sk_communications_breach/ [Visualizzato il 9 giugno 2015]

[63] I. Pogo (2013), Korean Court Orders SK Communications to Pay Damages to ID Theft Victims [online]. Disponibile al seguente indirizzo: http://www.databreaches.net/tag/sk-communications/ [Visualizzato il 9 giugno 2015]

[64] K. Vinton (2015), Premera Blue Cross Breach May Have Exposed 11 Million Customers' Medical And Financial Data [online]. Disponibile al seguente indirizzo: http://www.forbes.com/sites/katevinton/2015/03/17/11-million-customers-medical-and-financial-data-may-have-been-exposed-in-premera-blue-cross-breach/ [Visualizzato il 9 giugno 2015]

[65] B. Krebs (2015), Premera Blue Cross Breach Exposes Financial, Medical Records [online]. Disponibile al seguente indirizzo: http://krebsonsecurity.com/2015/03/premera-blue-cross-breach-exposes-financial-medical-records/ [Visualizzato il 9 giugno 2015]

[66] W. Ashford (2012), VeriSign admits security breach of corporate network [online]. Disponibile al seguente indirizzo: http://www.computerweekly.com/news/2240114786/Verisign-admits-security-breach-of-corporate-network [Visualizzato il 9 giugno 2015]

[67] J. Menn (2012), Key Internet operator VeriSign hit by hackers [online]. Disponibile al seguente indirizzo: http://www.reuters.com/article/2012/02/02/us-hacking-verisign-idUSTRE8110Z820120202 [Visualizzato il 9 giugno 2015]

[68] T. Greene (2012), FAQ about the VeriSign data breaches [online]. Disponibile al seguente indirizzo: http://www.networkworld.com/article/2185485/security/faq-about-the-verisign-data-breaches.html [Visualizzato il 9 giugno 2015]

[69] AOL, A Note to our Members [online]. Disponibile al seguente indirizzo: http://o.aolcdn.com/os/memberservices/faq.html [Visualizzato il 9 giugno 2015]

[70] AOL mail team (2014), AOL Security Update [online]. Disponibile al seguente indirizzo: http://blog.aol.com/2014/04/28/aol-security-update/ [Visualizzato il 9 giugno 2015]

[71] Reuters (2007), Monster.com Admits Keeping Data Breach Under Wraps [online]. Disponibile al seguente indirizzo: http://www.foxnews.com/story/2007/08/24/monstercom-admits-keeping-data-breach-under-wraps.html [Visualizzato il 9 giugno 2015]

[72] B. Bergstein (2007), Monster security breach teaches lessons [online]. Disponibile al seguente indirizzo: http://www.nbcnews.com/id/20534586/ns/technology_and_science-security/t/monster-security-breach-teaches-lessons/#.VXchc2BSW8p [Visualizzato il 9 giugno 2015]

[73] Secureinfo, THE TRW HACK [online]. Disponibile al seguente indirizzo: http://secureinfo.info/breaches/the-trw-hack [Visualizzato il 9 giugno 2015]

[74] Rome News Tribune (1984), Computer hackers steal code to credit rating bureau system [online]. Disponibile al seguente indirizzo: https://news.google.com/newspapers?id=ehwIAAAAIBAJ&sjid=hEUDAAAAIBAJ&dq=computer+hacker+%7C+hackers&pg=3014,3845383&hl=it [Visualizzato il 9 giugno 2015]

[75] M. J. Schwartz (2013), Yahoo Japan Data Breach: 22M Accounts Exposed [online]. Disponibile al seguente indirizzo: http://www.darkreading.com/attacks-and-breaches/yahoo-japan-data-breach-22m-accounts-exposed/d/d-id/1110035? [Visualizzato il 9 giugno 2015]

[76] K. Shubber (2013), Millions of users' data hacked in Yahoo Japan security breach [online]. Disponibile al seguente indirizzo: http://www.wired.co.uk/news/archive/2013-05/20/yahoo-japan-hacked [Visualizzato il 9 giugno 2015]