Cyber Risk:
risposta del mondo assicurativo

Alessia Venuto e Simone Radaelli
AIG Financial Lines Major Loss Adjuster Europe

Padova, 23 Luglio 2015

Cyber Risk: lo scenario attuale

Alessia Venuto
AIG
Financial Lines Major Loss Adjuster Europe

Cyber Risk: lo scenario attuale

AIG

Cyber Risk Overview

Preoccupazioni delle Organizzazioni

Le maggiori preoccupazioni dei clienti in merito ai “Cyber Risks”*

“Cyber risk” 86%

Danno property 80%

Danno nei confronti dei prestatori di lavoro 78%

Interruzione di attività 76%

Rischio di investimenti 76%

*Basato su un sondaggio AIG del 2012. Percentuale degli intervistati che indicavano di essere "molto" o "a volte" preoccupati su uno specifico rischio, su una base di 256 interviste tra broker, risk managers, IT managers

AIG

Preoccupazioni delle Organizzazioni

L'80% dei clienti ritiene che sia difficile fronteggiare le minacce cyber perché si evolvono troppo rapidamente

Il 74 % dei clienti ritiene che l'errore umano sia una fonte significativa di rischi cyber

L' 82% ritiene che gli hackers siano la prima fonte di minacce cyber

AIG

Lo scenario

- Il sondaggio AIG del 2012 evidenzia che le società sono preoccupate circa i rischi cyber e le violazioni dei dati
- I risk managers non stipulano polizze cyber perché gli IT departments sostengono che sia tutto sotto controllo
- La domanda di coperture cyber è aumentata del 33% nel 2012
- Solo il 20% delle società stipula polizze cyber nonostante sia la preoccupazione maggiore per l'86% dei nostri clienti

AIG

La "cyber security" è tra i programmi delle società?

- L'81% sostiene che il "senior management" da' un'alta priorità alle questioni di sicurezza
- Il 42% delle grosse organizzazioni non fornisce alcun training sulla sicurezza dei sistemi al proprio staff
- Il 33% delle grosse organizzazioni sostiene che le responsabilità per assicurare la sicurezza dei dati non sono chiare
- Il 93% delle società dove la policy in materia di sicurezza dei dati è poco conosciuta, subisce violazioni ad opera del proprio personale

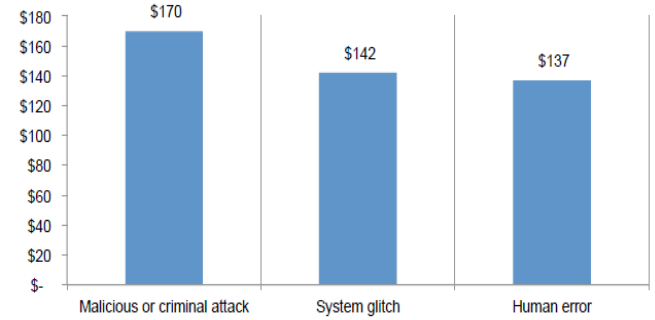
AIG

Claim Activity

Tipi di dati maggiormente esposti (*dal NetDiligence Claims Study 2013*)

- PII - informazioni personali identificabili (33% degli eventi)
- PHI - informazioni sanitarie protette (27% degli eventi)
- Informazioni su credit/debit cards (19% degli eventi)

Figure 5. Per capita cost for three root causes of the data breach
Consolidated view (n=350), measured in US$



Cause dei sinistri (*dal NetDiligence Claims Study 2013*)

- Hacker - Esterne (21% degli eventi)
- Furto/perdita dei PC (21% degli eventi)
- Malware/virus (19% degli eventi)
- Errore umano - mancanza di attenzione - impiegato negligente (75% degli eventi)

AIG

Aumento dei volumi di sinistri

Frequenza: volumi sinistri

USA

Dal 2011 al 2013 è aumentata del 154 %

2013 una violazione riportata ogni "business day"

2014 due violazioni per "business day" riportate ad AIG

EMEA

Un sinistro alla fine del 2013, 10 nel 2014

25 sinistri ad oggi nel 2015

AIG

Alcuni dati FERMA (Harvard Business Review), 2013

- Il 16,3% delle società ha un “chief information security officer”
- Il 20% delle società sostiene di avere un insufficiente budget per la sicurezza informatica
- Il 60% delle società non pianifica di assicurarsi
- 63.000 incidenti informatici in tutto il mondo nel 2014
- Numero tre volte superiore a quello registrato tre anni fa

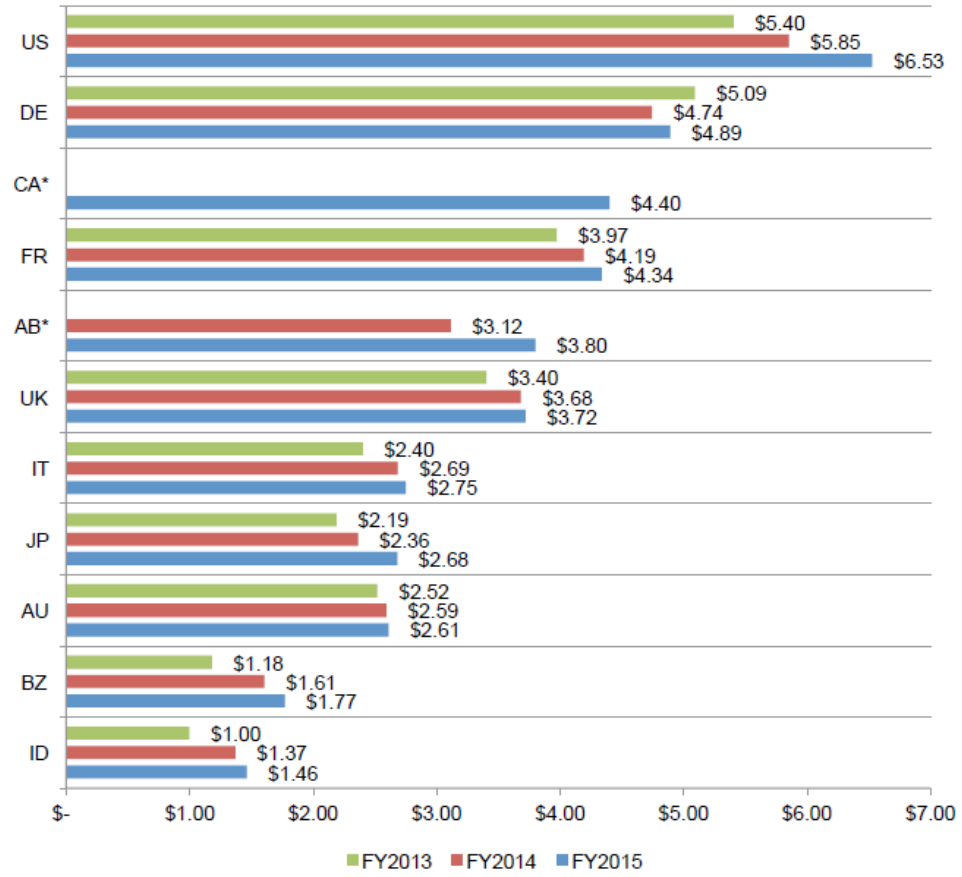
Alcuni dati: le 10 principali minacce contro la sicurezza e la privacy (FERMA), 2013

- Malware (72%)
- Administrative errors (48%)
- Incidents caused by third parties suppliers (34%)
- Malicious activity by employees (31%)
- Attacks against web (“DoS”) (30%)
- Theft or loss of mobile devices (28%)
- Internal hacker (26%)
- Terrorism (25%)
- Phishing attack (22%)
- Infiltration using mobile devices (20%)

AIG

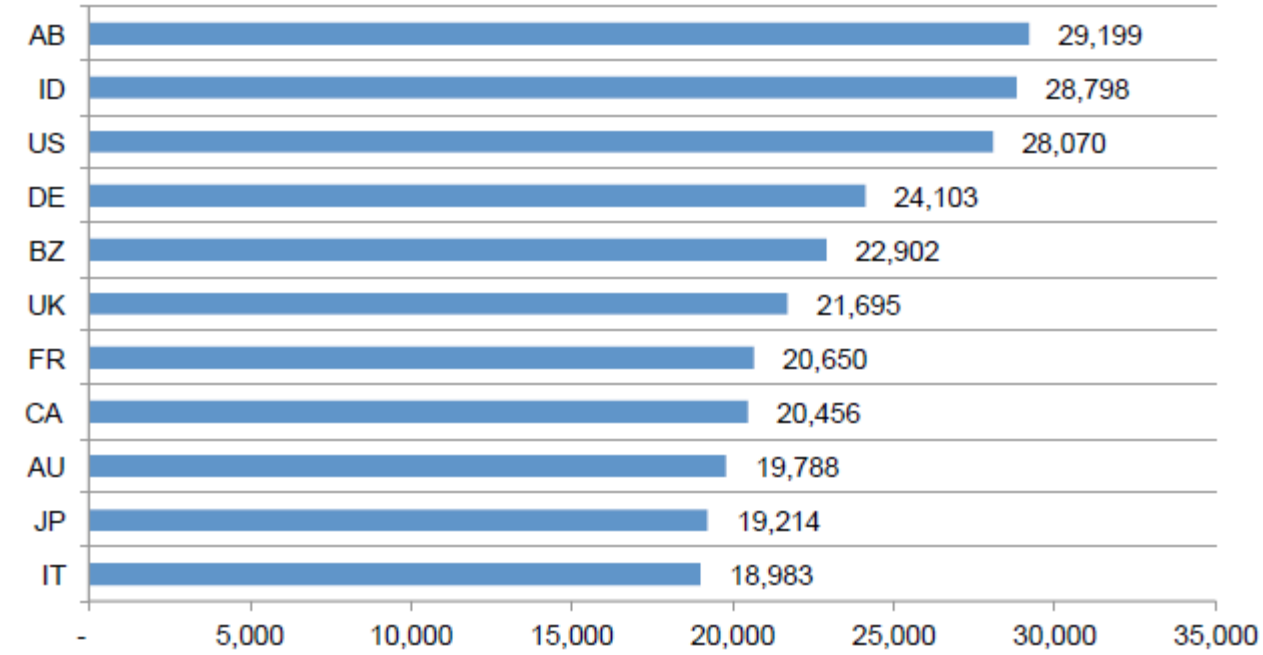
Claim Activity

Figure 2. The average total organizational cost of a data breach over three years
*Historical data is not available
Consolidated view (FY 2015 = 350, FY 2014 = 315, FY 2013 = 277)
Measured in US$ (millions)



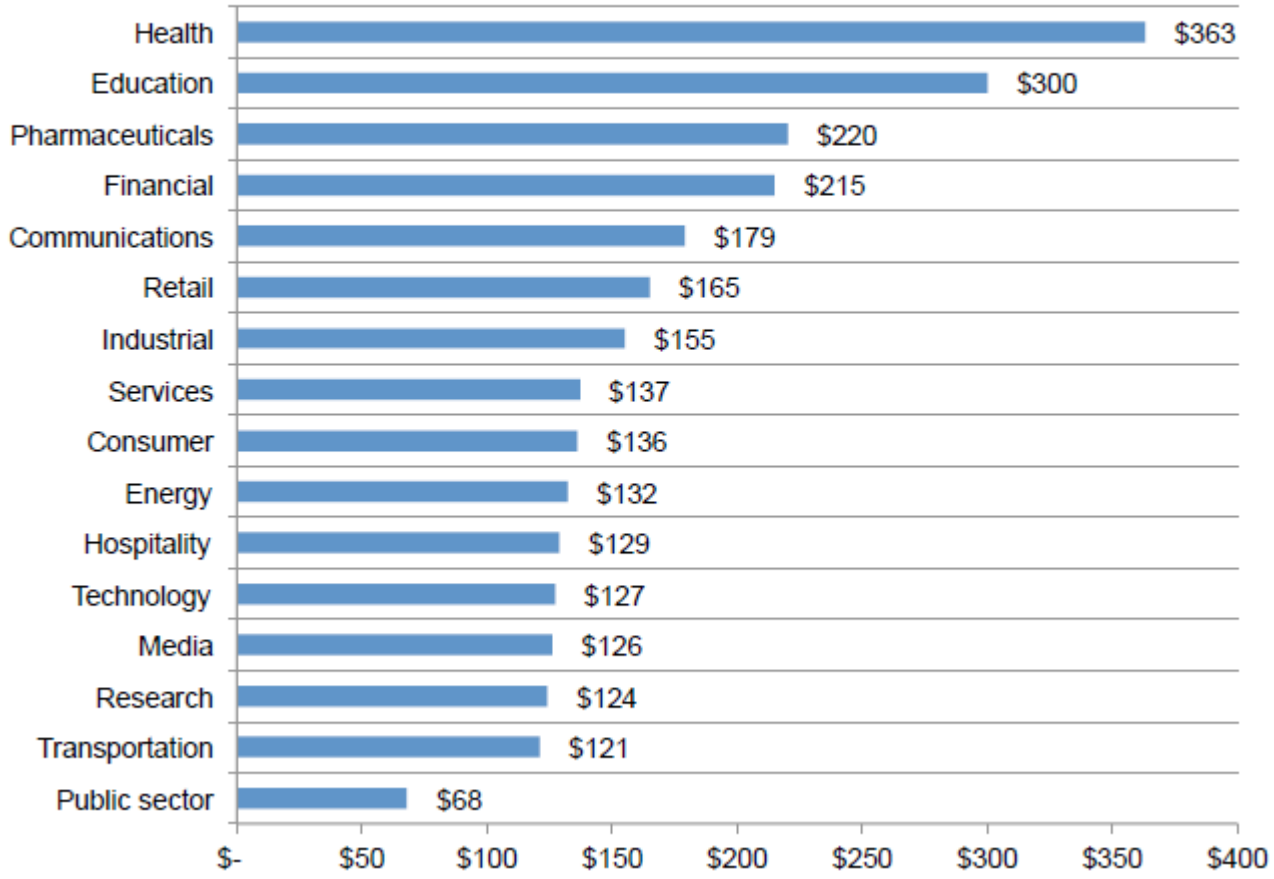
Claim Activity

Figure 3. The average number of breached records by country
Consolidated view (n=350)



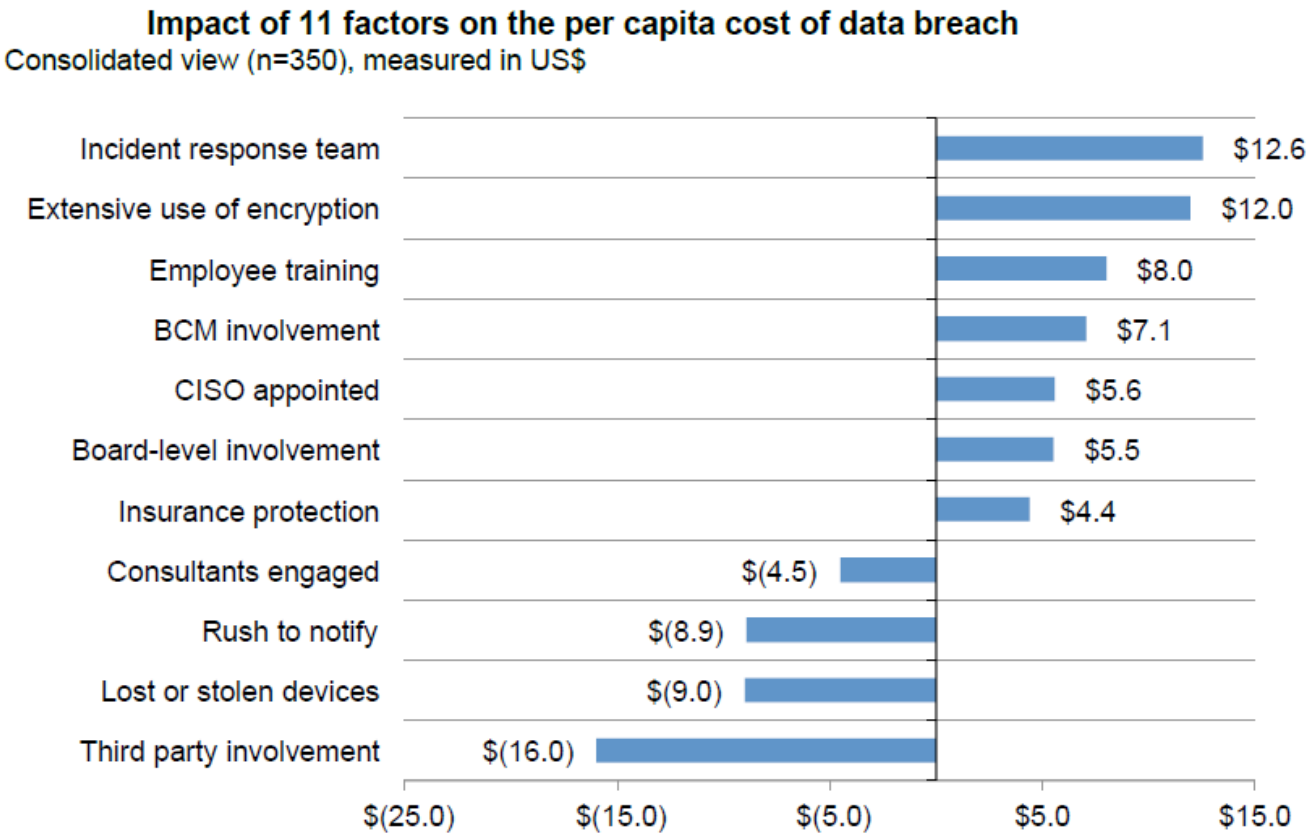
Claim Activity

Figure 4. Per capita cost by industry classification
Consolidated view (n=350), measured in US$



AIG

Claim Activity



Rischi delle banche derivanti da un attacco informatico e danni conseguenti

- Blocco o interruzione dei sistemi ICT
- Danno diretto
- Danno a terzi: violazione dei conti, mediante appropriazione credenziali clienti e accesso non autorizzato per scopi fraudolenti

AIG

Obblighi di prevenzione delle banche

- Adozione di sistemi di autenticazione al fine di evitare accessi non autorizzati
- Adozione di sistemi di avviso alla clientela sulle transazioni effettuate
- Monitoraggio di eventuali anomalie delle transazioni e relativo blocco delle stesse

AIG

Fattispecie Ricorrenti

Fattispecie ricorrenti

- **Danneggiamento**
  - ✓ Hacking/Cracking
  - ✓ Denial of service attack
  - ✓ Virus dissemination
  - ✓ Cyber terrorismo

- **Raccolta abusiva di dati**
  - ✓ Phishing
  - ✓ Furto di identità

AIG

Fattispecie ricorrenti

Furto di identità

Condotta illecita attuata attraverso un occultamento della propria identità mediante l'utilizzo indebito di atti concernenti l'identità e il reddito di un altro soggetto.

Conseguenze

- Sottrazione di denaro (90% dei casi)
- Danno alla reputazione

AIG

Fattispecie ricorrenti

Phishing

- Predisposizione di tecniche idonee a carpire fraudolentemente dati personali sensibili (user ID e password) al fine di accedere ai conti correnti di terzi

- Viene inviato ad un numero elevato di utenti della rete un messaggio di posta elettronica contenente un link che rinvia ad una pagina web clone di quella dell'istituto di credito

AIG

Fattispecie ricorrenti

Le fasi del phishing

- Planning – si decide chi colpire, quali tecniche usare, cosa sottrarre e per quali scopi
- Setup – si configurano i meccanismi per sferrare l'attacco e si raccolgono i contatti e le informazioni sulle vittime (per il tramite di siti che contengano grandi quantità di dati personali)
- Attack – si instaura il contatto con le potenziali vittime mediante diversi strumenti informatici o telematici, solitamente mediante email truffaldina
- Collection – vengono sottratte e raccolte le varie credenziali di accesso
- Fraud – si commerciano, vendono o si usano direttamente le credenziali per scopi fraudolenti
- Post attack – si cancellano le tracce dell'apparato predisposto per il phishing

AIG

Fattispecie ricorrenti

Pharming

Manipolazione degli indirizzi di DNS (domain name server) con l'obiettivo di indirizzare la vittima verso un server web clone appositamente attrezzato per carpire i dati personali di un terzo

- Modalità:

Installazione da parte dell'hacker sul computer della vittima di un virus in grado di reindirizzare il traffico verso un sito web fittizio

L'hacker altera il funzionamento di un server DNS portando più utenti a visitare inavvertitamente il sito fittizio, al fine di:

- ✓ installare virus sul pc dell'utente
- ✓ o raccogliere informazioni personali e finanziarie allo scopo di perpetrare furti di identità

AIG

Fattispecie ricorrenti

Man in the browser (MITB)

Forma di minaccia informatica relativa a:

MITM: intercettazione attiva delle comunicazioni, al fine di controllare l'intera comunicazione

MITB: intercettazione attiva delle comunicazioni volta a danneggiare gli istituti di credito ed i loro clienti, mediante inoltro alla banca di richieste di operazioni solo apparentemente provenienti dal cliente

AIG

Cyber Risk: le coperture

Simone Radaelli
AIG
Financial Lines Major Loss Adjuster Europe

Cyber Insurance : le coperture

AIG

Cyber Insurance – D&O

Cyber Insurance -D&O

Responsabilità patrimoniale personale dell'amministratore

Gli **amministratori** d'aziende sono, per legge e ovunque nel mondo, personalmente e solidalmente responsabili, con il proprio patrimonio, dei danni causati a terzi o alla società riguardo all'attività decisionale svolta per conto della stessa - doveri che discendono dalla legge e/o statuto sociale

Azione sociale di responsabilità (ex artt. 2932 e 2393 c.c.)
Azione dei soci di minoranza (art. 2393 bis c.c.).

Responsabilità verso i creditori (2394 c.c.) – Inosservanza degli obblighi inerenti alla conservazione dell'integrità del patrimonio sociale

Responsabilità verso i soci ed i terzi (2395 c.c.) – Singoli soci o terzi danneggiati direttamente *Presupposti: atto illecito dell'Amministratore nell'esercizio dell'ufficio* + *un danno diretto*

Sindaci (2407 c.c.) – **Dirigenti** (2396 c.c.)

AIG

Cyber Insurance - D&O

Casistiche di responsabilità degli Amministratori

Responsabilità per risk management e sistemi di controllo interni

Assicurare la protezione dei dati aziendali e assicurare che le informazioni e i dati personali siano preservati

Verificare il rischio aziendale (risk assessment) relativo ai *dati* → Sicurezza IT sia adeguata → Piano di risposta in caso di data breach → Staff training → Risk assessment dei providers → Cyber risks insurance

Fonte:Cyber risks: notes on a D&O perspective; RPC, Nov.2014

AIG

Cyber Insurance - D&O

In base a quanto previsto dal **Codice sulla privacy**, gli **amministratori** delle società devono individuare le **modalità di trattamento e protezione dei dati** personali.

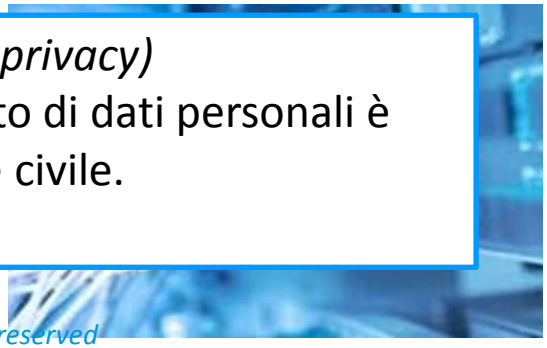
Il **collegio sindacale**, nonché i singoli sindaci individualmente, devono vigilare sulla conformità dell'operato degli amministratori alle prescrizioni del Codice sulla privacy.

In caso di violazione della tutela sulla privacy, **il soggetto leso** può

- rivolgersi al Garante della privacy proponendo apposito **ricorso, reclamo o segnalazione,**
- può proporre **ricorso direttamente al Tribunale ordinario**, dimostrando l'effettiva esistenza del danno subito e del nesso di casualità

Amministratori e sindaci (in solido) possono essere chiamati al risarcimento del danno derivante dalla violazione della normativa sulla privacy

Danni cagionati per effetto del trattamento(Art. 15 Codice privacy)
Chiunque cagiona danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell'articolo 2050 del codice civile.
E' risarcibile anche il danno non patrimoniale



AIG

Cyber Insurance - D&O
Potenziale responsabilità Amministratori

Coperture D&O e rapporti con eventi «Cyber»

- Costi di difesa in caso di procedimento del Garante / Costi interni per rispondere a procedimento Autorità
- Costi di difesa penale
- *Assicurato vs Assicurato – in alcuni casi, ove presente, potrebbe escludere l'azione da parte della Società ?*
- Terrorismo – cyber terrorist attack esclusione ?
- Danni alla persona

AIG

Cyber Insurance -D&O
Potenziale responsabilità Amministratori

2014 - Target Corporation

Gennaio 2014: Target annuncia sottrazione da paret di hackers di dati personali (inclusi nomi, indirizzi mail, numeri telefono) e informazioni su carte di credito di oltre 40 millioni di clienti.
Molte di queste informazioni su carte di credito sono state vendute dagli hackers al black market.

- ✓ **Class actions da parte dei clienti** : nel Marzo 2015 Target ha definito la class action promossa da diversi clienti riconoscendo un importo di 10 MUSD
- ✓ **Azione da parte di azionisti contro D&Os e contro l'Azienda**

Allegations: defendants were aware of how important the security of private customer information is to customers and to the company, as well the risks to the company that that a data breach could present. The complaints allege that the company "failed to take reasonable steps to maintain its customers' personal and financial information," and specifically with respect to the possibility of a data breach that the defendants failed "to implement any internal controls at Target designed to detect and prevent such a data breach."

- ✓ **Spesa di 61 MUSD per implementare anti-breach technology dopo l'attacco**
- ✓ Perdita di profitto - 46 % nel trimestre successivo all'evento.

Cyber Insurance - D&O
Potenziale responsabilità Amministratori

2008 - Wyndham Worlwide Corporation

- *2008 -2010* ***Hackers*** *sottraggono dati di carte di credito di oltre 600.000 clienti*
- *2012* **Azione da FTC** per mancata adozione misure di sicurezza
- *2012* **Azionisti** richiedono formalmente alla società di intentare una causa di responsabilità contro gli Amministratori per violazioni in tema di sicurezza dei dati.
  - Il Board, dopo aver incaricato uno Studio legale e dopo diversi meetings, sulla base delle conclusioni, non ha promosso la domanda di responsabilità.
- 2014: Azionisti ha avviato **derivative action** verso i membri del board che avevano respinto la richiesta.
  - 2014, La Corte ha **respinto l'azione** rilevando che la decisione del board era stata emessa dopo **adeguati accertamenti e indagini** (incarico a legale esterno, diversi meetings per discutere delle vicenda, analisi IT).

- Costi di difesa
- Security upgrades costs
- Consulente esterno nominato per rivedere IT security
- Wyndham ha chiesto ai propri providers impegni precisi in termini di standard

Cyber Insurance / Risk Assessment

Cyber Insurance /Risk Mgt.

Prior to suffering a data breach, **businesses should confer with knowledgeable counsel and technology consultants** to implement cybersecurity measures and compliance procedures.

Strong cybersecurity measures weaken any argument that a business or its management is reckless

Following a data breach, businesses must be prepared to respond to civil legal proceedings and government regulatory inquiries and investigations.

Management and/or the board of directors may have to defend the company's conduct in **parallel actions: a civil suit and a regulatory investigation.**

Defending its cybersecurity in a civil case while simultaneously identifying its cybersecurity flaws in a regulatory action places businesses in a tenuous, uncomfortable position, and is all the more reason to act diligently, prudently, and proactively before a breach occurs.

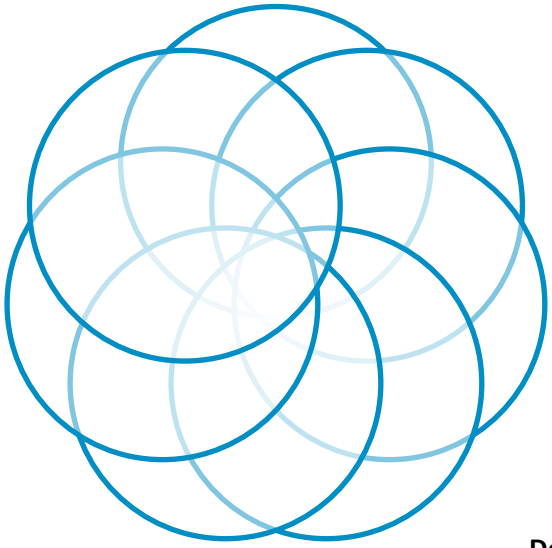
AIG

Cyber Insurance /Risk Mgt.

Guidance for Managing Cybersecurity **February 2014, the California Attorney General, in collaboration with the California Chamber of Commerce**

Risks item checklist summary of these practical recommendations for businesses on managing cybersecurity risks.

Form relationships with key third parties (e.g., law enforcement and cybersecurity experts) and have their contact information handy.



Prepare an incident response plan for when a cyber incident happens.

Prepare specific policies and procedures to implement in specific situations

Pick an incident team and assign a team leader; this team should include an executive and an in-house counsel if there is one.

Outline the basic steps of the incident response plan by **establishing checklists and clear action items**.

Define roles and responsibilities so that everyone is clear as to who is responsible for what should an incident arise.

https://oag.ca.gov/cybersecurity

AIG

Cyber Insurance /Risk Mgt.

Garante Privacy 2013

«Devono …essere adottate idonee e preventive **misure di sicurezza**, in modo da ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.»

«Il Codice prevede che per il trattamento dei dati è necessario che i titolari adottino

- **misure minime** di sicurezza che garantiscano, ad esempio, in caso di trattamento elettronico, la verifica e la convalida dell'identità di chi accede al sistema (identificativi personalizzati, password sicure…),
- l'adozione di un apposito sistema di autorizzazione che consenta solo specifiche attività predefinite, l'utilizzo di strumenti (come antivirus aggiornati e altri software e sistemi di protezione) per impedire accessi illeciti o abusivi che mettano a rischio l'integrità e la confidenzialità del dato personale.»

- **Bisogna poi essere pronti a gestire situazioni di crisi (….)**
- Occorre anche definire **misure di protezione particolari per i dati sensibil**i, tecniche crittografiche

AIG

Cyber Insurance – Coperture

Cyber Insurance / Triggers di Polizza

Violazione Dati Personali (Breach of personal information)

Difetti di Sicurezza (Security Failure)

Difetti di Sistema (System failure)

Cyber Insurance /Triggers di Polizza

A. Violazione Dati Personali *(Breach of personal information)*

*L'**accesso non autorizzato** o la **trasmissione non autorizzata** di Dati Personali per i quali la Società Assicurata è responsabile (Responsabile del Trattamento o Titolare del Trattamento - Legge Privacy)*

Dati personali	*Informazioni relative ad una persona fisica non di dominio pubblico e che permettano di identificare tale persona fisica (compreso il nome, l'indirizzo, il recapito telefonico o i dati clinici delle persone fisiche)*

Cyber Insurance /Triggers di Polizza

B. Difetti di Sicurezza (Security failure)

a) ***Intrusione*** *dovuta a difetto di sicurezza del Sistema Informatico della Società Assicurata, (inclusi: accesso e uso non autorizzato, un attacco che provochi interruzione di servizio o di accesso, la ricezione o trasmissione di un codice che esegue operazioni nocive, di software nocivi o virus…)*

➡ ***la distruzione, alterazione, corruzione, danneggiamento o cancellazione di Dati di Terzi*** *archiviati su qualsiasi Sistema Informatico della Società Assicurata*

a) ***Rivelazione di dati:***
- ✓ *dovuta a furto o alla perdita di hardware*
- ✓ *da parte di un dipendente della Società Assicurata*

Incluso furto password o codice accesso dai locali, dal Sistema informatico , ai danni di dirigente, amministratore o dipendente Società assicurata

AIG

Cyber Insurance /Triggers di Polizza

C. Difetti di Sistema (System failure)

*Un **atto od omissione negligente** da parte di un **dipendente** della Società Assicurata durante l'uso, la manutenzione o l'aggiornamento del Sistema Informatico della Società Assicurata*

- *Esclusi atti od omissioni durante manutenzione o l'aggiornamento di un Servizio Cloud o dispositivi elettronici di Terzi*

Cyber Insurance /Triggers di Polizza

❑ Definizione di Assicurato

*la **Società Assicurata***

***Persona Assicurata** = persona fisica - amministratore, un titolare dell'attività, un socio o un dirigente (ivi compreso Dirigente Responsabile) della Società Assicurata nella misura in cui la persona agisca in tale qualità*

*una persona fisica che è o è stata **dipendente** della Società Assicurata;*

*un **collaboratore esterno** sotto la direzione e supervisione del Contraente con riferimento ai servizi forniti al Contraente*

*ogni **erede o rappresentante** dell'Assicurato se richiesta relativa ad un atto, errore, o omissione del medesimo Assicurato.*

AIG

Cyber Insurance / Garanzie dirette

A - Gestione degli eventi

***Copertura delle spese** relative a*

1. Response Advisor (*Consulente di Reazione*) per i Servizi Legali
2. IT Services (*Esperto Informatico*) - Servizi di pronto intervento informatico
3. Consulente di Crisi
4. Ripristino dei Dati (*Data Restoration*)
5. Tutela della Reputazione (*Reputational Protection*)
6. Costi di Comunicazione (*Notification Costs*)
7. Monitoraggio del Profilo Creditizio e dell'Identità

➢ Limiti temporali

B - Istruttoria Privacy

Cyber Insurance / Garanzie

Response Advisor - Consulente di Reazione

Studio legale indicato in polizza interviene per la prestazione di **Servizi Legali**

- ✓ Recepisce le informazioni sull'evento e coordina gli altri soggetti (Esperto Informatico o del Consulente di Crisi)
- ✓ Segue adempimenti in tema di **obbligo di comunicazione** con eventuali **Autorità Amministrative** competenti
- ✓ la consulenza sulle comunicazioni ai **soggetti** («*Interessati*») i cui dati personali sono stati raccolti e trattati da o per conto della Società Assicurata
- ✓ il monitoraggio dei **reclami** presentati e la consulenza sulle risposte alle questioni sollevate dai soggetti di cui sopra
- ✓ la consulenza alla Società Assicurata sulla **reazione** della Società Assicurata in caso di eventi assicurati

AIG

C/M/S/ Law.Tax

NORTON ROSE FULBRIGHT

Matheson

Cyber Insurance / Garanzie

Esperto Informatico - IT Services

dimostrare se ha avuto luogo un Difetto di Sicurezza o Difetto di Sistema, le **modalità** con cui si è verificato e **se è ancora in corso**

rilevare se vi sia stata una Violazione di Dati Personali o una Violazione di Dati Societari e stabilire l'entità dei Dati Personali o dei Dati Societari eventualmente compromessi

limitare i Difetti di Sicurezza o Difetti di Sistema, ivi incluso il contenimento di attacchi diretti a determinare un'interruzione di servizio

AIG

Cyber Insurance / Garanzie

Consulente di Crisi (Crisis consultant)

Interviene per la copertura di **Tutela della Reputazione**

nominato dall'Assicuratore o dal Consulente di Reazione, per prestare **servizi di pubbliche relazioni o comunicazione** in caso di crisi

al fine di mitigare o evitare i potenziali effetti negativi o i danni reputazionali di un **Evento di Risonanza Pubblica**, ivi incluse la formulazione e la gestione di una strategia di comunicazione.

Cyber Insurance / Garanzie

Ripristino dei dati (Data Restoration)

spese relative ai casi di Difetto di Sicurezza o Difetto di Sistema per:

- ✓determinare se i Dati possano o meno essere ripristinati o ricreati;
- ✓ricreare i Dati non siano leggibili da computer o siano corrotti;
- ✓caricare e personalizzare nuovamente il software in licenza

Cyber Insurance / Garanzie

Costi di comunicazione:

- spese relative all'indagine, raccolta di informazioni, preparazione e comunicazione ai Soggetti Interessati e/o a qualsiasi Autorità Amministrativa competente in caso Violazione di Dati Personali o Violazione di Dati Societari

Monitoraggio del Profilo Creditizio e dell'Identità:

- servizi di monitoraggio del profilo creditizio e del furto d'identità, volti a rilevare possibili usi impropri di Dati Personali in caso di Violazione di Dati Personali

Dati societari si intendono segreti commerciali, dati, documenti soggetti a segreto professionale o altre informazioni, ecc di Terzi, non disponibili al pubblico.

AIG

Cyber Insurance / Garanzie

B - Istruttoria Privacy:

✓ Costi di Difesa relativi a **Istruttorie di un'Autorità Amministrativa**.

Azione, indagine, richiesta o controllo formale o ufficiale da parte di un'Autorità Amministrativa nei confronti di un Assicurato…

a) l'Assicurato sia stato **identificato** per iscritto dall'Autorità Amministrativa,
b) derivante **dall'uso o dal sospetto uso improprio di Dati Personali** o da qualsiasi altro aspetto relativo al **controllo o al trattamento di Dati Personali**, anche tramite delega attribuita ad un Fornitore Esterno di Servizi
c) che sia **disciplinata dalla Legislazione Privacy**,

Esclusioni
- richiesta o azione che interessi l'intera industria **non relativa ad una sola impresa**
- le azioni, indagini, richieste o i controlli formali riguardanti una **violazione dolosa** della Legislazione Privacy**.**

Autorità Amministrativa = un Garante della Privacy o un'autorità pubblica costituita secondo la Legislazione Privacy in qualsiasi giurisdizione e che ha il potere di dare esecuzione coattiva agli obblighi legali relativi al trattamento o al controllo dei Dati Personali (o, ove pertinente, dei Dati Societari)

AIG

Cyber Insurance /Garanzie

C - Liability

Copertura per **danni a terzi** e **costi di difesa** dell'Assicurato in caso di Richi**este di Risarcimento** da parte di Terzi riconducibili a

Violazioni di Dati Personali o **Violazioni di Dati Societari** da parte dell'Assicurato

Difetti di Sicurezza

per **omessa comunicazione ai Soggetti Interessati e/o all'Autorità Amministrativa** da parte della Società Assicurata di una Violazione di Dati Personali in conformità agli obblighi della Legislazione Privacy.

per responsabilità della Società Assicurata e derivino da effettive o asserite **violazioni di obblighi del Detentore dei Dati** relativi al trattamento per conto della Società Assicurata dei Dati Personali e/o dei Dati Societari (di cui la Società Assicurata sia responsabile)

Cyber Insurance / Liability

Richiesta di risarcimento

la ricezione o la notifica da parte dell'**Assicurato** di:

- ✓ una **domanda scritta** con la quale si rivendica un risarcimento dei danni; o
- ✓ un **procedimento civile o amministrativo** inteso a ottenere una tutela legale, il rispetto della legge o l'irrogazione di una sanzione.

Definizione di «*Terzi*»

entità giuridica o una persona fisica con esclusione di

- Assicurati,
- Fornitori Esterni di Servizi
- Detentori dei Dati
- ogni altra entità o persona fisica che abbia un interesse finanziario o un ruolo gestionale nella Società Assicurata

Cyber Insurance / Liability

Danni coperti

- ✓ Decisioni, sentenze emesse contro l'**Assicurato**;
- ✓ danni punitivi o esemplari, se assicurabili per legge;
- ✓ somme di denaro che l'**Assicurato** deve pagare in seguito a transazione (autorizzata dalla Compagnia) in relazione ad una **Richiesta di Risarcimento**.

Esclusione: risarcimenti che non hanno funzione compensativa

Cyber Insurance / Liability

Costi di Difesa

gli onorari, i costi e le spese ragionevoli e necessari che l'Assicurato sostiene, con il preventivo consenso scritto dell'Assicuratore, in relazione all'indagine, alla risposta, alla difesa, in relazione ad una Richiesta di Risarcimento (o istruttoria di una Autorità Amministrativa).

I Costi di Difesa non comprendono la remunerazione dell'Assicurato, del Fornitore Esterno di Servizi o del Detentore dei Dati, il costo del tempo da essi impiegato o altri costi o spese generali dell'Assicurato, del Fornitore Esterno di Servizi o del Detentore dei Dati

Cyber Insurance / Principali Esclusioni

Danni alla Persona o a Cose (perdita o distruzione di beni materiali, diversi da Dati).

Responsabilità Contrattuale qualsiasi garanzia, dichiarazione, impegno, clausola contrattuale o responsabilità assunta o accettata da qualsiasi **Assicurato** ai sensi di un qualsiasi contratto o accordo

Condotte intenzionali se commessi da amministratori, soci, dirigente responsabile e dipendenti che agiscono con tali soggetti *>> Costi di difesa anticipati sino ad accertamento giudiziario*

Sinistri riconducibili a guerra, invasione, eccetto **Terrorismo Informatico**

Guasto elettrico o meccanico delle infrastrutture, diverse dal **Sistema Informatico della Società Assicurata**

Ripristino di sistemi, procedure o software difettosi laddove la presenza di difetti, carenze, vulnerabilità agli attacchi o intrusioni era stata comunicata/rilevata in anticipo da evitare l'eventuale **Perdita** che ne consegua o ridurne l'impatto

Cyber Insurance /Additional coverage Network Interruption

Network Interruption loss

Copre i danni al Sistema subiti in caso di interruzione del Sistema Informatico della Società Assicurata:

(i) dopo la scadenza del Waiting Hours Period (X hours) e durante l'Interruzione > limite di x giorni;

(ii) per un massimo di y giorni a decorrere dalla risoluzione dell'Interruzione

- Retention di polizza

Interruption and Mitigation costs

Costi di Blocco del Sistema sostenuti una volta trascorsa metà del Periodo di Carenza per ridurre la durata di un'Interruzione Significativa del Sistema Informatico della Società Assicurata.

Cyber Insurance /Additional coverage Network Interruption

Costi di blocco del sistema - Network interruption Costs

- i costi e le spese ragionevoli e necessari che la Società Assicurata sostenga per ridurre la durata di un'Interruzione del servizio prestato

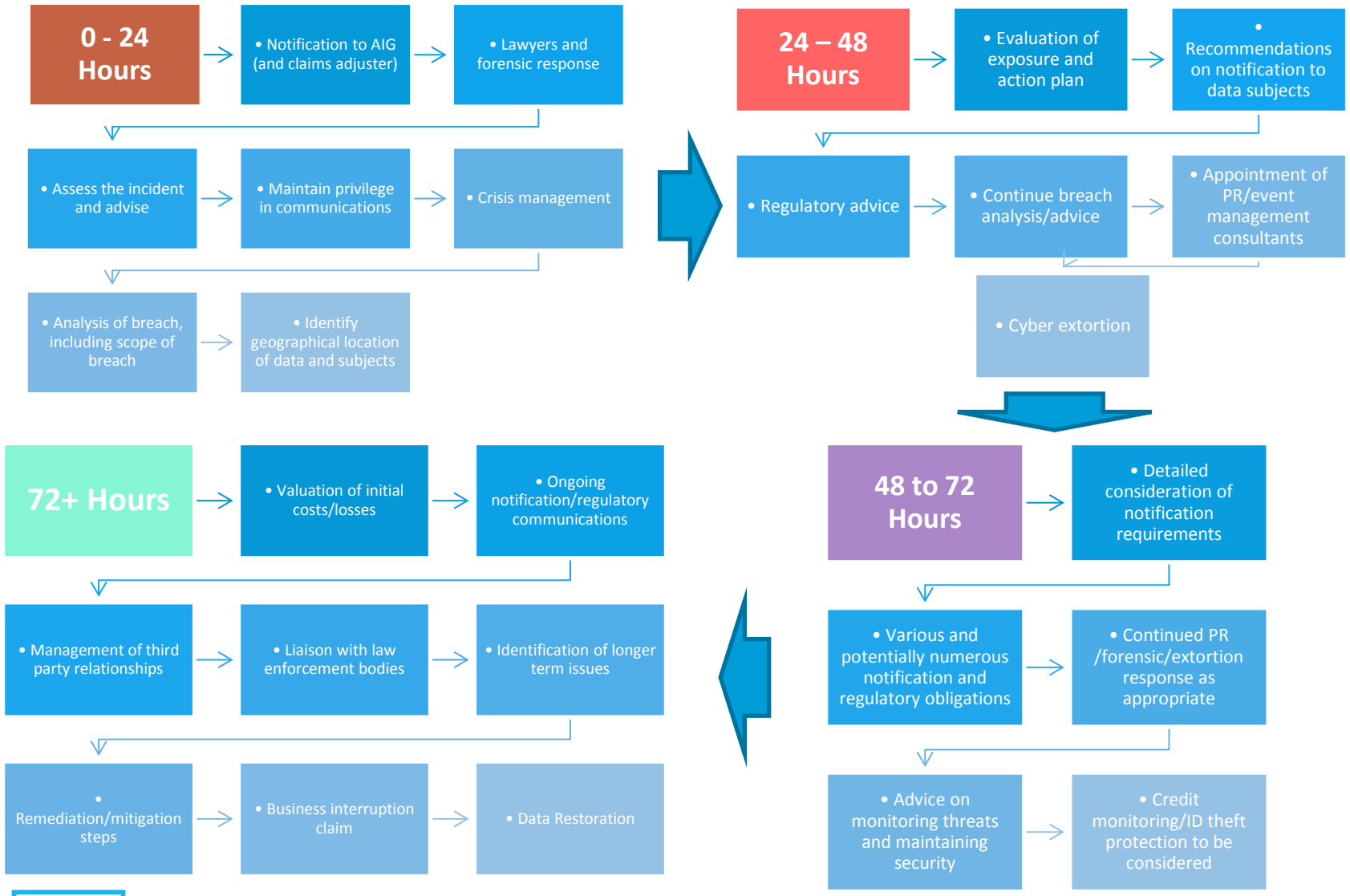
Danno al sistema - Network loss

- la riduzione dei profitti netti che, senza Interruzione, la Società Assicurata avrebbe guadagnato (e che è attribuibile ad una perdita di ricavi).
- le spese sostenute dalla Società Assicurata, volte ad assicurare la continuità delle normali procedure operative della Società Assicurata.

➢ Retention di polizza

Cyber Insurance

LIFECYCLE OF A CYBER CLAIM



AIG

Claims examples – Case studies from AIG

Esempi di sinistro

AIG in EMEA ha visto in uguale numero

Difetti di sicurezza

- Difetti di sicurezza che originano da DoS, hacking, malware
- Attacchi da indirizzi IP russi e cinesi
- Attacchi mirati da parte di hackers che violano i legacy systems

Difetti di sistema

- Errori da parte di dipendenti
- Difetti dei software
- Normalmente consistenti in violazione di informazioni personali o societarie

AIG

Esempi di sinistro

Errore umano - UK

- Sinistro in cui le informazioni personali sono state inavvertitamente inviate a più di 4000 dipendenti della stessa compagnia

- Sinistro in cui 250 clienti di un rivenditore online hanno ricevuto un'email erroneamente inviata a tutti gli indirizzi che risultavano visibili, senza nascondere i destinatari della mailing list

AIG

Esempi di sinistro

Errore umano

- Uno studio legale invia per errore documentazione ad un terzo
- Il terzo conferma per iscritto che avrebbe distrutto i dati ricevuti
- La corrispondenza inviata conteneva limitate informazioni confidenziali
- Il Cliente è stato informato e non ha avanzato una richiesta di risarcimento

AIG

Esempi di sinistro

Hacker/ Extortion

- Società di viaggi
- Violazione del dicembre 2014 – sospettato un ex dipendente
- IT director riceve una sua riproduzione con un cappio ed un link ad un' URL che mostrava i dati dei clienti
- Si trattava di dati non attuali
- Coinvolta la polizia francese
- L'evento appariva connesso ad un precedente incidente – problematiche relative a non disclosure/limite aggregato

AIG

Esempi di sinistro

Cyber extortion

- L’assicurato subisce un blocco del servizio
- Minaccia di far saltare il sistema
- Incaricati esperti
- Il colpevole non è stato identificato ma il servizio è stato ripristinato
- Polizza ha coperto parzialmente le spese legali
- BI coverage non impegnata perché il *waiting time* non è stato superato

AIG

Esempi di sinistro

Società che fornisce assistenza medica/assistenza viaggio

- Assicurato UK che forniva assistenza medica/viaggio in 70 paesi
- La società presta servizio per governi ed enti non governativi
- Per 5 giorni i sistemi informatici sono risultati fuori uso
- L'assicurato è stato allertato dalla società esterna deputata a monitorare i siti web degli hackers
- Un mese dopo, una seconda violazione dei sistemi informatici
- A tutti i titolari dei dati è stata data la notifica della violazione del sistema e contestualmente offerta una polizza personale sul furto dell'identità e un controllo dei movimenti (credit monitoring and theft insurance)
- Danno di circa GBP 1M

AIG

Esempi di sinistro

Impiegato disonesto (esempio USA)

- Assicurato è una banca multinazionale
- Il senior financial analyst, della divisione prestiti, ha scaricato più di 2 milioni di records
- Venduti 20.000 profili ogni settimana per USD 500 ciascuno
- Notifica richiesta per più di 10 milioni di persone
- 42 class actions
- Danno totale subito dall' assicurato USD 40 milioni
- La polizza ha coperto l'intero massimale pari a USD 20 milioni

AIG

Esempi di sinistro

Hacker

- Grosso rivenditore USA
- Violazione del dicembre 2013
- Danno scoperto dai servizi segreti
- *Malware* scoperto su 43.750 POS
- Su un periodo di 20 giorni, *malware* ha sottratto informazioni in merito alle carte di credito e debito (inclusi i PIN) di 40 milioni di clienti
- E' stato successivamente scoperto che gli hackers hanno violato il database, accedendo ad informazioni personali di ulteriori 70 milioni di clienti

AIG

Esempi di sinistro

Hacker

- Assicurato subisce un *denial of service attack* da un indirizzo IP russo
- Sito fuori uso per circa 1 ora
- Dopo il ripristino un cliente effettuando il log-in vede i dettagli degli altri clienti e pubblica gli screen shot su Twitter
- Dati rimossi dall'assicurato (a seguito di negoziazione con il cliente)
- Indirizzo IP russo bloccato
- Solo 2 records compromessi
- No richieste

AIG