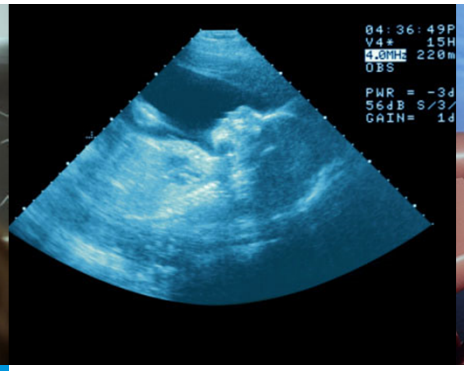
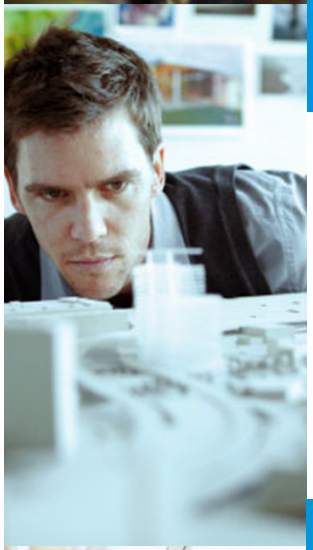
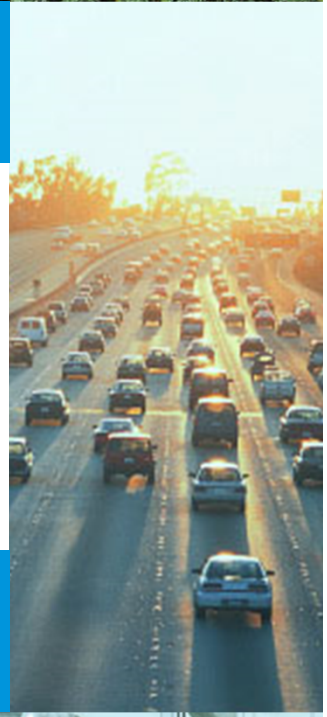
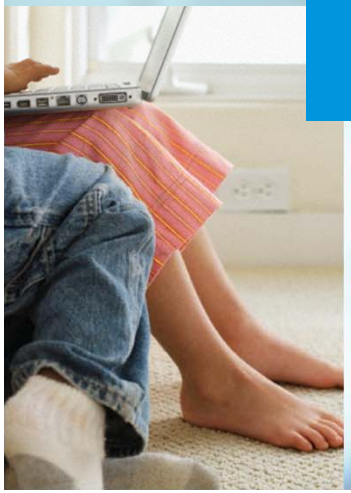
CyberEdge

I rischi informatici: come difendersi?


I dati hanno un’importanza fondamentale nella nostra quotidianità

Sono oggetto di attenzione dei criminali

> Costo dei Cybercrimes nel 2011 per le società: circa USD 388Mld [1]

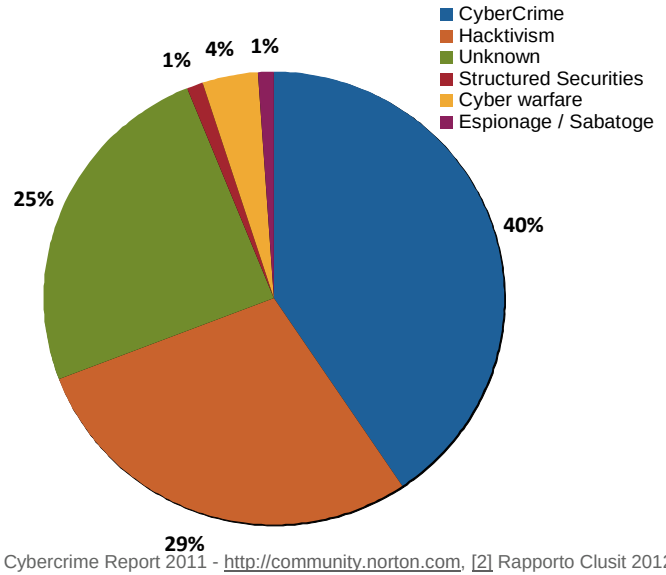
> Ricavi Cybercrimes: 7/12 miliardi USD [2]

> Media: un crimine online ogni 19 secondi [3].

> Minacce alla sicurezza: 32% da hacker e criminalità organizzata, 19% da infedeltà dei propri dipendenti (in aumento), 49% furto di sistemi informatici portatili (laptop, hard disk e memory stick non protette da idonea crittografia) [4].

> Maggior singola somma rubata (ad oggi nota): 14.8 Milioni USD [6]

Attacchi significativi classificati per tipologia 1° QT 2012: [5].



ATTACCANTI PER TIPOLOGIA	2011	1Q 2012	Totale
Cybercrime	170	175	345
Unknown	148	122	270
Hacktivism	114	106	220
Espionage / Sabotage	23	3	26
Cyber warfare	14	17	31
TOTALE	469	423	892

[1] Norton Cybercrime Report 2011 - http://community.norton.com, [2] Rapporto Clusit 2012 [3] Lockton Report Feb. 2012, [4] Lockton Report Feb. 2012 (citaz NetDiligence – Study of cyber and data breach insurance claims – June 2011 - http://www.netdiligence.com, [5] e [6] Rapporto Clusit 2012

Sono oggetto dell'attenzione del legislaltore europeo

A livello europeo

Proposta (gen. '12) normativa organica (tutela uniforme) - self applicable che prevede la totale revisione della 95/46/CE:

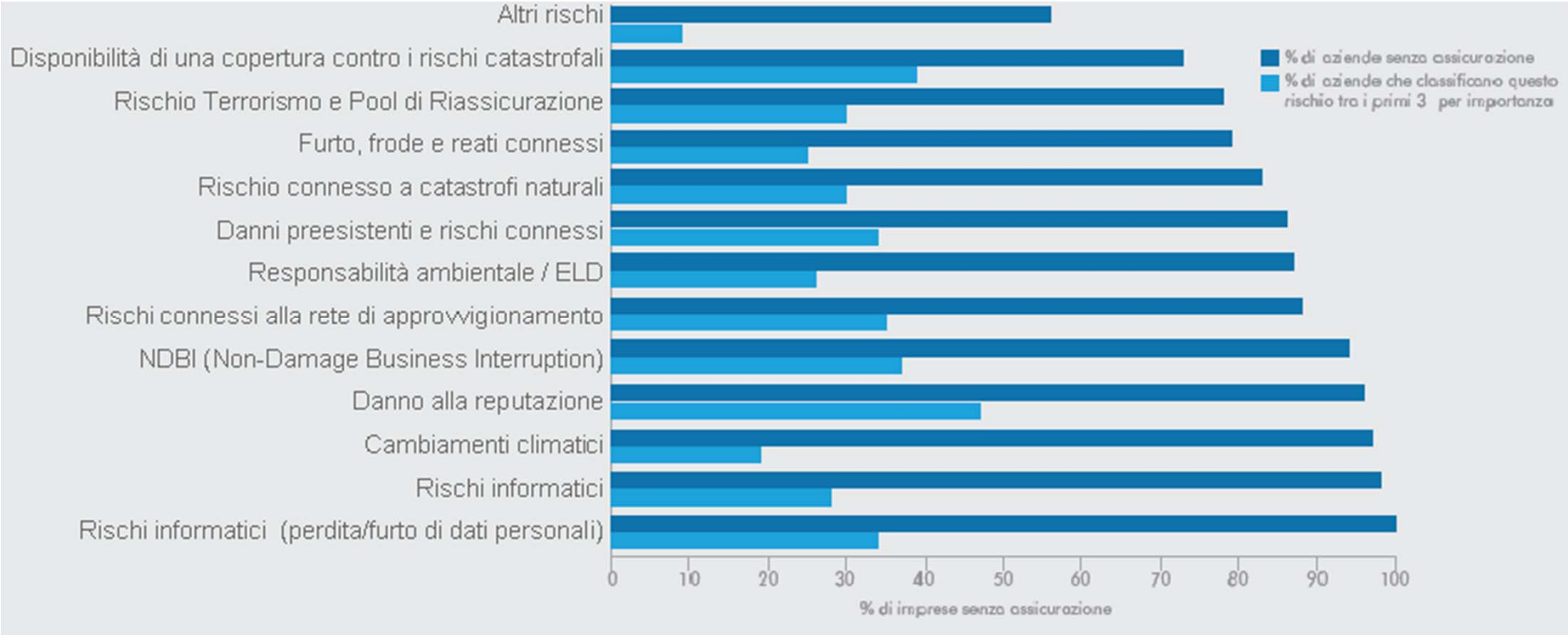
- Applicabilità a tutti coloro che gestiscono dati personali di cittadini europei per uso affari
- Nuovi principi di trasparenza e riservatezza
- Obblighi di nominare un Responsabile
- Obblighi di comunicazione entro 24 ore
- Nuove azioni civili specifiche
- Azioni amministrative: sanzioni fino a 1 milione di euro per gli individui e fino al 2 % del fatturato globale per le società che non rispettino la normativa.

A livello italiano

La normativa di riferimento è il D.Lgs. 196/2003 intitolato «Codice in materia di protezione dei dati personali», noto anche come «Testo unico sulla privacy» che ha sostituito la Legge 675/1996

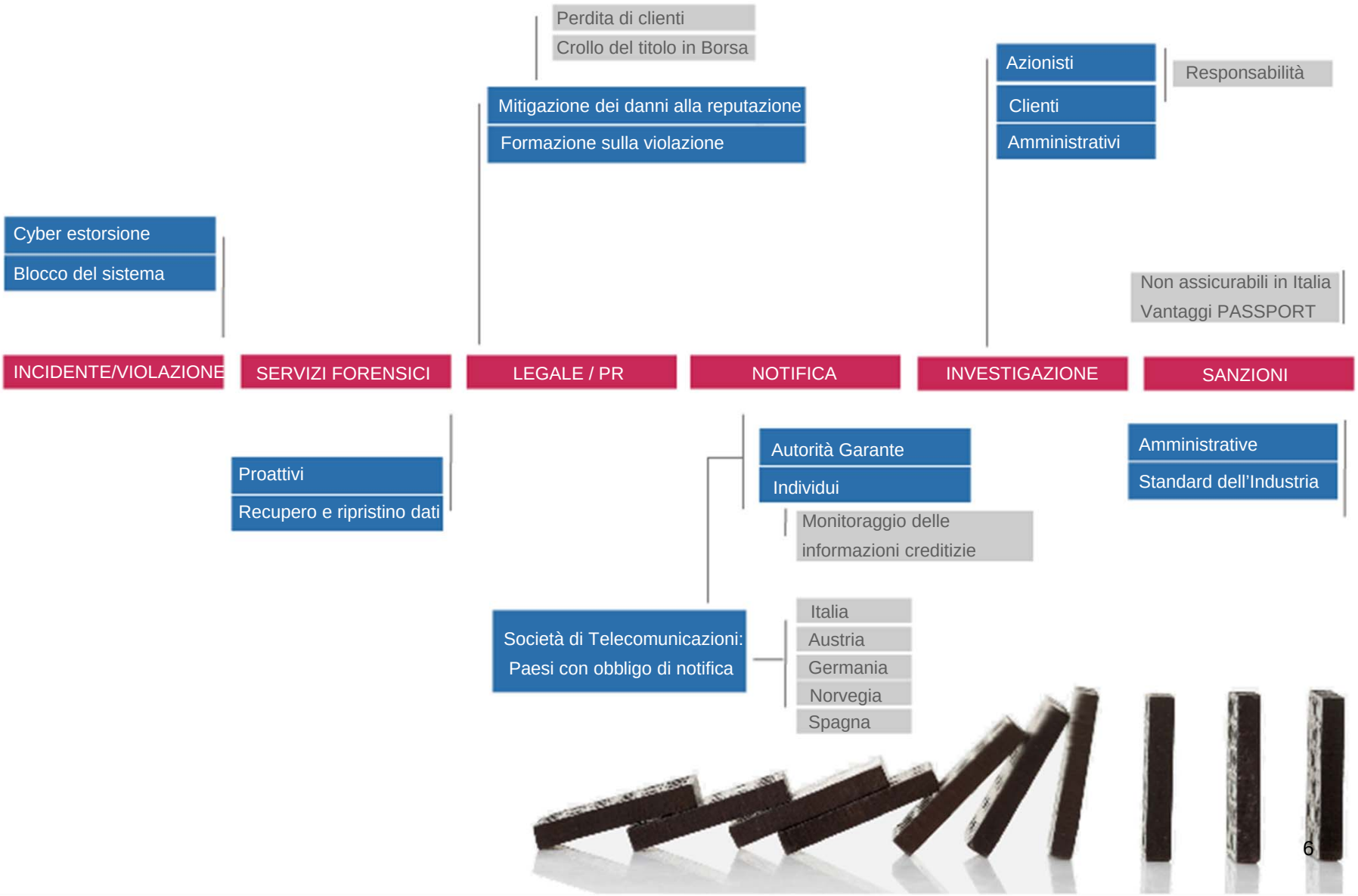
Eppure facciamo poco per difenderli

Sondaggio: Rischi Prioritari - Assenza Di Copertura



È STATO CHIESTO A 101 *RISK MANAGER* DI INDIVIDUARE I PRIMI 3 RISCHI CHE CONSIDERANO PRIORITARI E DI INDICARE SE È STATA STIPULATA UNA CORRISPONDENTE COPERTURA ASSICURATIVA. AIRMIC GIUGNO 2012

L’evoluzione di un sinistro



CyberEdge

COPERTURE STANDARD

A. RESPONSABILITA' RELATIVA AI DATI

> **A.1** Perdita di Dati Personali (RC TERZI)

> **A.2** Perdita di Dati Societari (RC TERZI)

> **A.3** Outsourcing (RC TERZI)

> **A.4** Sicurezza della Rete (RC TERZI)

B. ASSISTENZA IN CASO DI ISTRUTTORIA AMMINISTRATIVA

> **B.1** Istruttorie Amministrative relative a Dati

C. DANNI REPUTAZIONALI E COSTI DI REAZIONE

> **C.1** Servizi di Difesa Tecnica Preventiva

> **C.2** Ripristino della Reputazione della Società Assicurata

> **C.3** Ripristino della Reputazione Individuale

> **C.4** Comunicazione ai Soggetti Interessati

> **C.5** Monitoraggio

> **C.6** Dati Elettronici (Danni propri)

MODULI OPZIONALI

D. Responsabilità per Attività Multimediali (RC TERZI)

E. Estorsione con Minaccia Relativa al Sistema Informatico (Danni propri)

F. Blocco del Sistema (Danni propri)

A - RESPONSABILITA' RELATIVA AI DATI : # 1

A 1 -Perdita di Dati Personali, A 2 - Perdita di Dati Societari, A 3 - Outsourcing

Il risarcimento dei danni cagionati a terzi in relazione ad un'asserita o effettiva violazione dei Dati Personali e/o dei Dati societari anche in relazione violazione di un obbligo dell'Outsourcer come conseguenza di:

- accesso non autorizzato o la trasmissione da parte di un Assicurato di Dati Personali per i quali la Società Assicurata sia responsabile, in ragione della sua qualità di Responsabile del Trattamento, o di Titolare del Trattamento come definito dalla Legislazione Privacy applicabile.
- rivelazione accidentale e/o colposa da parte di un Assicurato di Dati Societari per la quale la Società Assicurata sia responsabile.
- accesso non autorizzato, la trasmissione e/o la rivelazione accidentale e colposa, da parte di un Outsourcer, di Dati Personali e/o Dati Societari per i quali la Società Assicurata sia responsabile.

A - RESPONSABILITA' RELATIVA AI DATI : # 2

A4 - Sicurezza della Rete

Risarcimento dei danni cagionati a terzi conseguenti a atti, errori od omissioni dell'Assicurato che abbiano determinato come esito:

- Contaminazione dei dati di terzi da software non autorizzato, codici computerizzati, virus specificamente pensati per danneggiare i sistemi informatici dell'Assicurato
- Impossibilità per un terzo di accedere ai propri dati
- Furto codici di accesso alla rete di un terzo
- Furto materiale hardware dell'Assicurato
- Distruzione delle banche dati presenti sui sistemi informatici dell'Assicurato dovuta ad una falla nella rete di sicurezza
- Rivelazione non autorizzata di dati dovuta a violazione della Sicurezza

B - Assistenza in caso di Istruttorie amministrative

- **La criticità:**

  Il rispetto della normativa applicabile nei differenti paesi richiede importanti investimenti da parte della società ed a volte non sono comunque sufficienti a garantire l'ottemperanza di norme applicabili in continua evoluzione e/o un'esaustiva risposta alle richieste avanzate dalle Autorità in caso di incidente e/o mancato trattamento degli stessi conforme agli standard

- **La soluzione offerta:**

  Costi di consulenza, investigazione e difesa avanti alle Autorità con la possibilità di accedere a servizi di legali e consulenti selezionati da AIG in tutte le giurisdizioni

C - Misure di Contenimento della Crisi

Servizi a Valore aggiunto

DANNI REPUTAZIONALI E COSTI DI REAZIONE

C1 - Servizi forensi pro-attivi (c.d Proactive forensic services)

Costi per verificare e, se del caso, contenere e certificare, anche ai fini dell'utilizzo in Tribunale, se vi sia stata o sia in corso una violazione della sicurezza dei dati.

AIG e suoi consulenti offriranno una assistenza immediata al fine di :
a) verificare in che modo si sia verificata una violazione della sicurezza e

b) la causa della violazione; quindi quantificheranno l'impatto della violazione e la tipologia di dati violati, per consentire a AIG e l'Assicurato di decidere un proporzionale livello di risposta.

C2 e C3 - Ripristino della reputazione della Società e/o individuale

Costi per reagire all'eventuale pubblicità negativa derivante dalla diffusione di notizie circa la violazione della sicurezza dei dati

Un esperto sarà a disposizione per assistere i Clienti con riferimento a tutte le conseguenze di una violazione dei dati, e per coordinare gli sforzi, in termini di pubbliche relazione, che possano essere necessari. Il cliente potrà accedere contemporaneamente a questo servizio e a quello offerto dagli esperti di Sicurezza informatica.

C - Misure di Contenimento della Crisi

Servizi a Valore aggiunto

C4 – Comunicazione ai soggetti interessati (obbligatoria per società di Telecomunicazioni)

- Indagini e preparazione delle comunicazioni all'Autorità Garante ed ai soggetti interessati da una violazione di dati.

C5 - Monitoraggio

- Costi per servizi di monitoraggio volti a prevenire l'uso improprio di Dati Personali come conseguenza di un'effettiva o asserita Violazione della sicurezza dei dati o violazione della legislazione sulla Privacy.

C6 - Dati Elettronici ***"Danni propri"***

- Determinazione se i dati detenuti per conto di un terzo possano essere ripristinati o rigenerati
- Rigenerazione e recupero per le ipotesi in cui i sistemi di back up non li abbiano salvati, ovvero questi siano stati corrotti o perduti a causa di una carenza tecnica, o per negligenza o inadempienza di un operatore o di un'altra persona legittimamente incaricata allo scopo.

Modulo opzionale #1:
Responsabilità per attività multimediali

Richiesta di Risarcimento e relativi costi di difesa derivanti, nell'esecuzione o nella mancata esecuzione di Attività Multimediali, per:

i. diffamazione
ii. violazione non intenzionale di un diritto d'autore
iii. plagio, pirateria o appropriazione indebita o furto di idee o informazioni;
iv. violazione delle norme relative ai diritti di pubblicazione e sfruttamento dell'immagine
v. concorrenza sleale, ma solo se contestata insieme con uno degli atti elencati nei punti da (i) a (iv) sopra; o
vi. atto che determini una responsabilità derivante dalla negligenza dell'Assicurato in relazione a qualsiasi contenuto multimediale digitale**.**

Modulo opzionale #2: *“Danni propri”*

Cyber Extortion – Estorsione con minaccia al sistema informatico

Indennizzo per i Danni che un Assicurato subisca come conseguenza esclusiva di una Minaccia alla sicurezza.

La copertura include qualsiasi:

i. somma di denaro pagata da un Assicurato, con il preventivo consenso scritto dell’Assicuratore, per prevenire o mettere fine ad una Minaccia di Estorsione; e

ii. gli Onorari Professionali da sostenersi affinché consulenti esterni conducano un’indagine per determinare la fondatezza della Minaccia di Estorsione.

Modulo opzionale #3: *“Danni propri”*
Blocco del sistema

- **Copertura del danno diretto - perdita di profitto - subito dalla società in caso di violazione della sicurezza che richieda un’interruzione significativa e/o la sospensione dei servizi prestati dai sistemi informatici**
- **Franchigia**: La copertura inizia a operare trascorse 8/12 ore dalla sospensione/interruzione (periodo di carenza)

Principali esclusioni*

- Antitrust
- BI/PD
- Responsabilità contrattuale
- Reati, dolo e atti volontari
- Rischio dati connesso a dichiarazioni inesatte e/o reticenti in sede di sottoscrizione del rischio
- Raccolta dati illegale
- Rischi inassicurabili per legge
- Proprietà intellettuale (salvi carve back)

* Per l'elenco dettagliato delle esclusioni raccomandiamo di far esclusivo riferimento al normativo di polizza

Criteri di Quotazione

Nella quotazione del rischio CyberEdge i principali elementi valutati possono così sintetizzarsi:

- Tipologia di attività della Cliente (hazard grade)
- Fatturato
- Split geografico
- Standard di sicurezza dati adottati dalla Cliente
- Massimali & Franchigia
- Storia sinistri
- Moduli opzionali

Caso emblematici italiani

Settembre 2010: Tentativo di Phishing

Anonimo server canadese invia migliaia di e-mail a dirigenti e funzionari di comuni, comunità montane, ministeri, ambasciate,consolati e distretti militari avvisandoli di una grave minaccia alla sicurezza e della necessità di procedere all'adozione di misure di sicurezza contenute in una "procedura" allegata che altro ovviamente non era che un eseguibile contenente un virus potenzialmente dannoso ed in grado di compromettere l'integrità dei database e/o trasmetterne il contenuto all'esterno. Il successo dell'attacco era basato sull'utilizzo dio un indirizzo e-mail apparentemente attendibile: ced-sogei-ancitel@sogei.it.

Fonte: www.ilsole24ore.com/art/norme-e-tributi/2010-09-15/attacco-online-canada-italiana-100017.shtml?uuid=AYwRI4PC

Gennaio 2013: Attacco Hacker al Tribunale di Milano

Il sito del Tribunale di Milano è stato recentemente oggetto di attacco: al posto dell'Homepage è stata visualizzata l'immagine riportata a lato che riportava il segunete messaggio" *Hacked by LndTm 2013 Italian crew" (cioè Formazione italiana), una maschera tricolore di V for vendetta, usata solitamente da Anonymous. Sotto l'immagine la scritta «preparatevi ha inizio l'Apocalisse! È la fine per un nuovo inizio. Sta arrivando come l'ira di DIO il vero cambiamento per i giovani*"

Fortunatamente non sembrerebbero essere state violate le banche dati del tribunale ma possiamo comunque percepire la pericolosità di un simile episodio.

Fonte: http://www.ilsole24ore.com/art/notizie/2013-02-16/tribunale-milano-hacker-150537.shtml?uuid=AbObW4UH

Crimes e tendenze: casi emblematici

#1: Spionaggio e sabotaggio anche supportato da Governi nazionali (es. operazione Olympic Games, il virus Stuxnet [1])

#2: 2011: il caso Sony

La Multinazionale dell'Entertainment nel 2011 e stata oggetto di ripetuti attacchi; ha perso il 30% della Mkt Cap, ha visto sottratti 100 milioni di profili completi degli utenti sottratti dal network dei videogiocatori e dalla piattaforma di *Online, Entertainment*, ha dovuto sospendere per 24 giorni l'erogazione di giochi online (utilizzati da 77 milioni di utenti) [2]

#3: Febbraio 2011: Le società di sicurezza

il CEO di un'importante società di sicurezza, contractor di importanti aziende americane e dello stesso governo, ha annunciato di essersi infiltrato con successo nel gruppo Anonymous; per ritorsione è stato "linciato" pubblicamente con violazione del suo profilo Twitter, rivelazione online del suo indirizzo, numero di telefono e numero di assistenza sanitaria e, soprattutto, è stata violata la rete aziendale con sottrazione/pubblicazione di 68 mila e-mail riservate anche di contenuto imbarazzante.[3]

#4: Febbraio 2013: Attacco hacker alla Jeep su Twitter

Falsi tweet dall'account ufficiale del marchio Fiat: «Il marchio ceduto alla Cadillac». I pirati informatici hanno sfruttato l'account per lanciare falsi messaggi. Come quello che annunciava la cessione della società alla Cadillac. Con una nota ufficiale Jeep ha spiegato di aver ripreso il controllo del profilo un'ora dopo l'attacco [4].

[1] Rapporto Clusit 2012 - fonte NYT [2] Rapporto Clusit 2012 – http://attrition.org/security/rant/sony_aka_sownage.html0 [3] Rapporto Clusit 2012 – http://it.wikipedia.org/wiki/Anonymous#Attacco_alla_HBGary_Federal [4] http://motori.corriere.it/motori/tecnologia/13_febbraio_20/jeep-attacco-hacker_e2c9aada-7b41-11e2-ba69-3fd719869bcf.shtml

Esempi sinistri notificati a AIG

 # 1 - Dipendente infedele:

Il caso

L'Assicurato (un rivenditore) è stato chiamato in causa da un concorrente a causa dell'appropriazione indebita da parte di un impiegato di dati confidenziali del concorrente.

Definizione del sinistro da parte di AIG US

Il sinistro è stato definito e pagato con un esborso di circa $200,000.

 # 2 - Hacking:

Il caso

Alcuni Hacker hanno forzato l'accesso ai sistemi informatici di una catena di hotel ubicati in 26 diverse locazioni accedendo ai nominativi ed ai numeri di carte di credito di circa 480.000 clienti.

Definizione del sinistro da parte di AIG US

Rimborso all'assicurato di $980,000 per spese di gestione della crisi.

 # 3 - Errore/Negligenza (Istruttoria da parte dell'Autorità):

Il caso

L'assicurato ha accidentalmente reso disponibili informazioni confidenziali riguardanti 42.000 studenti sul proprio sito web. I genitori di uno studente hanno avanzato la minaccia di una possibile class action affermando che vi era state una violazione della privacy di proprio figlio e che l'assicurato era stato negligente non avendo protetto in modo adeguato la privacy degli studenti. Inoltre la Federal Trade Commission ha iniziato un'istruttoria per determinare se l'assicurato abbia rispettato il FTC Act che proibisce false dichiarazioni in merito alla privacy.

Definizione del sinistro da parte di AIG US

Pagati circa $250,000 in costi di difesa nel processo istruttorio iniziato dall'Autorità.

Esempi sinistri notificati a AIG

 # 4 - Perdita/Furto materiale di attrezzature:

Il caso

L'assicurato ha perso supporti alcuni informatici contenenti informazioni sensibili (cartelle cliniche) e numeri di assistenza sanitaria.

Definizione del sinistro da parte di AIG US

Rimborso all'assicurato di $400,000 per servizi di call center e costi di monitoraggio delle identità "perse". Altre spese sono oggetto di definizione.

 # 5 - Dipendente disonesto

Il caso

Un dipendente di una grossa consumer reporting agency (agenzia che raccoglie informazioni sui consumatori) sottrae le informazioni personali di milioni di clienti.

Definizione del sinistro da parte di AIG US

• costi sostenuti per esperti forensi incaricati di stabilire quali siano i dati trafugati e a quali persone appartengano.

• costi sostenuti per informare i milioni di persone i cui dati sono stati sottratti

• costi connessi ad attività di credit monitoring per accertare che le vittime del furto non registrino ammanchi a seguito del sinistro

• parcelle del consulente incaricato di preparare l'azienda ad affrontare un'eventuale indagine

• costi di assistenza legale e di difesa nell'ambito del procedimento intentato nei confronti dell'azienda

• risarcimenti di danni in caso di decisione sfavorevole all'azienda

Esempi sinistri notificati a AIG

Il caso

 # 6 - PERDITA DI DATI IMPUTABILE A FORNITORE ESTERNO

Il server di postaelettronica e l'hard disk di un'azienda sono stati sottratti mentre erano affidati ad un fornitore esterno

Definizione del sinistro da parte di AIG

• costi sostenuti per esperti forensi incaricati di stabilire quali siano i dati trafugati e a quali persone appartengano.
• costi sostenuti per informare i soggetti interessati dal furto di dati
• costi connessi ad attività di credit monitoring per accertare che le vittime del furto non registrino ammanchi a seguito del sinistro
• parcelle del consulente incaricato di preparare l'azienda ad affrontare un'eventuale indagine
• parcelle dei consulenti PR incaricati di assistere l'azienda nelle operazioni di comunicazione esterna a seguito del sinistro.

 # 7 - HACKING – CARTE

Il caso

Il sistema informatico di una società di trattamento dei pagamenti con carte di credito subisce un attacco hacker che compromette la sicurezza dei dati delle carte di credito

Definizione del sinistro da parte di AIG

• costi sostenuti per esperti forensi incaricati di stabilire quali siano i dati trafugati e a quali persone appartengano.
• costi sostenuti per informare i milioni di persone i cui dati sono stati sottratti
• costi connessi ad attività di credit monitoring per accertare che le vittime del furto non registrino ammanchi a seguito del sinistro
• costi sostenuti per consulenti di PR al fine di attenuare il danno alla reputazione aziendale a seguito del sinistro
• parcelle del consulente incaricato di preparare l'azienda ad affrontare un'eventuale indagine
• costi di assistenza legale nell'ambito dell'indagine condotta dalle autorità competenti
• costi di assistenza legale e di difesa nell'ambito del procedimento intentato nei confronti dell'azienda

American International Group, Inc. (AIG) is a leading international insurance organization serving customers in more than 130 countries and jurisdictions. AIG companies serve commercial, institutional, and individual customers through one of the most extensive worldwide property-casualty networks of any insurer. In addition, AIG companies are leading providers of life insurance and retirement services in the United States. AIG common stock is listed on the New York Stock Exchange and the Tokyo Stock Exchange.

AIG is the marketing name for the worldwide property-casualty, life and retirement, and general insurance operations of American International Group, Inc. Products and services are written or provided by subsidiaries or affiliates of American International Group, Inc. Not all products and services are available in every jurisdiction, and insurance coverage is governed by actual policy language. Certain products and services may be provided by independent third parties. Insurance products may be distributed through affiliated or unaffiliated entities. Certain property-casualty coverages may be provided by a surplus lines insurer. Surplus lines insurers do not generally participate in state guaranty funds and insureds are therefore not protected by such funds.