Nuove forme di rischio per persone e aziende relativamente al cyber crime: il danno reputazionale

Mario Dusi
Avvocato in Milano e Monaco di Baviera

Il Cyber Crime

Il cyber crime o crimine informatico è *un crimine commesso utilizzando un computer, una rete o un dispositivo hardware*.

Il computer o il dispositivo può essere l'agente, il mezzo, il complice o l'obiettivo del crimine. Un crimine può avere luogo sul solo computer o in combinazione con altre posizioni e luoghi.

L'impatto del cyber crime nel mondo digitale è un problema in forte crescita e rappresenta

il rischio del futuro:

non riguarda solo i professionisti connessi alla rete e che operano online, ma rende tutti meno sicuri: e-commerce, istituzioni pubbliche, aziende, organizzazioni, associazioni e consumatori

Valore del crimine: *ogni anno le conseguenze degli attacchi informatici costano al comparto business mondiale circa 445 miliardi di dollari, il 50% dei quali pesa sulle 10 maggiori economie mondiali (stima* Banca Mondiale, 2016).

Stima dei costi, ad oggi, gravanti sulle imprese, per le necessarie riparazioni conseguenti agli attacchi informatici sono, in media, 492 mila euro per grandi imprese e 33 mila euro per piccole e medie imprese (PMI).

Paesi più colpiti: *USA (108 miliardi di dollari/anno), Cina e Germania. Al quarto posto, il Brasile, con 7,7 miliardi di dollari di perdite annuali. In coda, l'Italia per cui i danni da cyber crime ammonterebbero a 900 milioni di dollari (report di AGCS,* Allianz Global Corporate & Specialty, settembre 2015).

I settori economici maggiormente colpiti: energia, utilities (trasporti, sanità), impianti chimici ed industria mineraria (50%), seguiti dai servizi finanziari, dal manifatturiero e dai servizi professionali.

Il Cyber Crime

Il crimine informatico può consistere in un **singolo evento**, *se visto dalla prospettiva della vittima.*

Trojan Horse: keystroke logger, ovvero un programma che registra quanto viene digitato sulla tastiera.

Esempi:
• il **phishing** (attività finalizzata ad estorcere dati personali - in prevalenza legati alle carte di credito od ai conti bancari - attraverso una richiesta esplicita al suo legittimo possessore), **il furto** e **la manipolazione di dati o servizi tramite azioni di hacking o virus**, il **furto di identità**, le **frodi bancarie o legate all'e-commerce**.

• il **ransomware**, che utilizzando diversi strumenti per l'hacking di pubblico dominio, bloccano i file della vittima (criptandoli) e/o sottraggono la disponibilità dei dati, al fine di chiedere un riscatto (generalmente richiesto in cyber monete quali bitcoin o moneypak) per il ripristino della situazione preesistente (Cyber estorsione).

• l'attacco **DDos,** che ha lo scopo di rendere un server, un servizio o un'infrastruttura indisponibile, sovraccaricando la banda passante del server o utilizzando le risorse fino ad esaurimento.

Altri esempi di crimine informatico che consiste in una **serie continua di eventi/contatti**, sono:
• il **cyber stalking e le molestie, le molestie ai minori, l'estorsione, il ricatto, la manipolazione dei mercati finanziari, lo spionaggio e le attività terroristiche**

I danni derivanti da Cyber Crime

Il crimine informatico espone aziende e privati a notevoli rischi di danno, molti dei quali difficili da quantificare in termini finanziari:

1) Danni materiali: danneggiamento, furto, uso illecito e vendita di dati interni, dei clienti e dei fornitori, violazione della privacy, distruzione di computer, server, macchinari etc.

Alcuni esempi:
• Il furto di dati relativi a un'importante trattativa commerciale o vendita di una società quotata in Borsa possono causare danni enormi alla società oggetto di attacco (affare sfuma apparentemente senza motivo).

• La manipolazione del mercato borsistico attraverso l'intrusione nelle reti delle aziende quotate, in quelle dei loro avvocati o revisori, per carpire (e poi adeguatamente diffondere, magari attraverso chat o social network) report finanziari, informazioni su fusioni e acquisizioni, piani di ristrutturazione ecc. al fine di alterare la quotazione in Borsa.

2) Danni economici → i costi di ripristino, di acquisto di nuovi macchinari, risarcimenti danni, pagamento di penali, spese legali, riduzione del fatturato, riduzione dell'efficienza operativa in seguito al blocco delle attività e degli impianti, risarcimento di danni a terzi, pagamento di multe/penali, costi di miglioramento dell'infrastruttura IT, di assunzione di nuovi specialisti, costi che derivano dalla mancata chiusura di contratti e quelli legati all'aumento delle polizze assicurative, spese di consulenza da parte di esperti in pubbliche relazioni, per attenuare i rischi alla reputazione e di revisori contabili.

I danni derivanti da Cyber Crime

3) Danni "ultra" economici
Ad Esempio: l'attacco informatico rivolto alla rete elettrica Ucraina il 23 Dicembre 2015, primo caso di interruzione di fornitura di energia elettrica dovuto ad un cyber crime, che ha cagionato un blackout dell'intera regione Ivano-Frankivsk (interruzione della fornitura di energia elettrica per 225.000 persone), infliggendo un pesante danno al paese.
In pratica, gli hacker, dopo aver rubato le credenziali degli operatori della linea, hanno inviato un malware (malicious software) tramite un allegato di Microsoft Office che ha completamente danneggiato il sistema.

4) Danni "collaterali", tra i quali la motivazione dei dipendenti, le sanzioni delle autorità di vigilanza ed, ad esempio, i danni derivanti dallo smarrimento di un server spedito via aerea e contenente i dati aziendali per l'avvio di una filiale estera.

5) Danni immateriali come i danni reputazionali, i danni all'immagine sia verso l'interno che verso l'esterno, la perdita di clienti, di quote di mercato, di competitività, di opportunità di business, la violazione della privacy e l'impossibilità dell'azienda di continuare la sua attività (business interruption).

Il Danno Reputazionale

La reputazione è:

1) **Personale**: onore e decoro di ogni persona (indipendentemente dall'attività che svolge)
2) **Professionale:** dignità e prestigio della persona nell'ambiente /settore lavorativo

La reputazione è un diritto:

a) inviolabile della personalità, assoluto, indisponibile e imprescrittibile (diritto soggettivo perfetto)
b) riconosciuto e tutelato dall'art. 2 Costituzione e dall'art. 595 Cod. Pen.
c) la cui lesione comporta un **DANNO RISARCIBILE:**

   a) sia **patrimoniale, ex art. 2043 c.c.,** che **non patrimoniale ex art.2059 (morale)**, suscettibile di quantificazione equitativa ex art. 1226 c.c. e, in relazione al danno non patrimoniale, **a prescindere dalla prova della commissione di un reato**

   a) anche in favore delle persone giuridiche ed enti (soggetti per i quali non è, per loro natura, configurabile un coinvolgimento psicologico in termini di patema d'animo): ogniqualvolta vi sia lesione di una situazione giuridica del soggetto in questione e il fatto lesivo incida su diritti che rappresentino l'equivalente di diritti fondamentali della persona umana, costituzionalmente garantiti (*Cass. Sezione III n. 12929 del 4 giugno 2007*)

Provata la lesione del diritto alla reputazione, **il diritto al risarcimento del danno** consegue alla prova che il fatto lesivo ha cagionato un perdita patrimoniale o un danno non patrimoniale (in caso di lesione alla reputazione **sia personale che professionale) *c.d. danno conseguenza*** *(Cass. S.U. dell'11 novembre 2008 n. 26972, Cass. Civ. del 13 novembre 2015 n. 23206 , Cass. Civ. del 29 gennaio 2016 n. 1651)*

→ *Superato l'orientamento del c.d. danno evento, con risarcimento in re ipsa senza l'ulteriore prova della sua esistenza*

Il Danno Reputazionale

In Italia, il Danno Reputazionale è il rischio maggiormente temuto dalle Aziende quale conseguenza di Cyber Crime (65% delle aziende)

Oggi, infatti,

RETE

- Transazioni commerciali, acquisti e vendite, pagamenti
- Reperimento di informazioni su persone, aziende, prodotti e servizi
- Recensioni rispetto all'operato di aziende, ai loro beni e servizi, che possono influenzare e orientare – in positivo o in negativo - il consumatore
- Fondamentale il ruolo delle Reti Social, canale importante di comunicazione, in grado di veicolare la "buona" come la "cattiva" immagine di un'azienda o di specifici prodotti e servizi

Un attacco cyber costituisce, infatti, una **situazione di "crisi"** che **rischia di compromettere la fiducia dei consumatori e creare danni oltre le previsioni.**

La gestione della crisi deve integrare processi, attività, meccanismi decisionali e piani di comunicazione finalizzati:

a) a preservare la continuità del business
b) a ridurre gli impatti economici, sociali e reputazionali derivanti dall'evento critico

Come è perseguito legalmente Cyber crime?

Legislazione italiana

1.1 La prima vera normativa contro i cyber crimes è stata la **Legge 547/93** ("*Modificazioni ed integrazioni alle norme del Codice Penale e del Codice di Procedura Penale in tema di criminalità informatica*").

Precedentemente:
Legge 191/78 che introduceva nel Cod. Pen. l'art. 420, attentato ad impianti di elaborazione dati; Legge 121/81 prima forma di tutela dei dati archiviati in un sistema informatico; Legge 197/91 indebito utilizzo delle carte di credito; Legge 518/92"pirateria informatica".

Con la **Legge 547/93** si introducono, nel Codice Penale, **fattispecie di reati che riguardano 4 aree di interesse**:
1) **Frodi informatiche**: art 640 ter ("Frode informatica)"

2) **Falsificazioni**: art. 491-bis ("Documenti informatici")

3) **Integrità dei dati e dei sistemi informatici**: art. 635-bis ("*Danneggiamento di sistemi informatici e telematici*"); 635-ter ("*Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità*"; 635-quater ("*Danneggiamento di sistemi informatici o telematici*"); art. art. 392 comma 3 ("*Esercizio arbitrario delle proprie ragioni con violenza sulle cose*"); art. 615-quinquies ("*Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico*");

4) **Riservatezza dei dati e delle comunicazioni informatiche:** art. 615-ter ("*Accesso abusivo ad un sistema informatico o telematico*"); art. 615-quater ("*Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici*"); art. 621 ("*Rivelazione del contenuto di documenti segreti*"); art.617-quater ("*Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche*"); art. 617-quinquies ("*Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche*"); art. 617-sexies ("*Falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche*"); art. 623-bis ("*Altre comunicazioni e conversazioni*");

Come è perseguito legalmente Cyber crime?

Legislazione italiana

1.2 D.Lgs. 231/2001, che estende la responsabilità delle persone giuridiche, delle società e delle associazioni, anche prive di personalità giuridica, ai reati informatici per la mancata predisposizione preventiva di misure idonee ad evitare che dipendenti o collaboratori interni delle stesse commettano tale tipologia di illeciti.

1.3 Aprile 2013 Provvedimento (c.d. "data breach") dell'Autorità Garante per la protezione dei dati personali dell'obbligo, per le aziende di telecomunicazioni e fornitori di servizi internet italiane, di comunicare entro 24 ore ogni episodio che possa comportare la perdita, distruzione o la distribuzione indebita di dati sensibili

Normativa Comunitaria

Necessaria, per garantire l'efficacia della normativa nazionale, considerata l'"territorialità" del crimine informatico.

a) **Convenzione del Consiglio d'Europa di Budapest sulla criminalità informatica del 23 novembre 2001,** in vigore dal 2004, ratificata in Italia con la **Legge 18 marzo 2008, n. 48**, che ha introdotto ulteriori modifiche al Cod. Pen., recependo ulteriori reati oltre a quelli disciplinati dalla L. 547/1993.

b) **Decisione Quadro 2005/222/GAI del 24 febbraio 2005**, in materia di reati informatici a livello europeo, finalizzata ad armonizzare e rendere effettiva la cooperazione a livello transnazionale, al fine di poter combattere il cyber crimine

c) **2013**, la Commissione Europea ha costituito **l'European Cybercrime Centre**, presso il quartier generale dell'Europol all'Aia (informazioni, prevenzione e reazione rispetto ad attività illegali online compiute dalla criminalità organizzata, l'e-banking e altre attività finanziarie online, lo sfruttamento sessuale dei minori online).

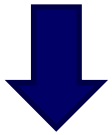
d) **Regolamento Europeo sulla Privacy,** che entrerà in vigore nel 2017

Nonostante la normativa civile e penale per la tutela dei danni,
in pratica,
in caso di Cyber crime,

non potendosi individuare uno specifico e determinato "convenuto",

nella maggior parte dei casi, a livello globale,
DETTO CRIMINE RIMANE IMPUNITO,

con conseguente impossibilità di accertamento e liquidazione GIUDIZIALE dei danni, compreso il Danno Reputazionale



Come ci si protegge dal rischio di danno da Cyber Crime?

*Secondo la **Global Economic Crime Survey 2016 di PWC** presso un campione significativo di aziende italiane):*

- *il 20% delle imprese è stata vittima del cyber crime almeno una volta negli ultimi 2 anni.*

- *Secondo il 60% delle aziende, il cyber crime arriva soprattutto dall'esterno e viene identificato soprattutto in hacker, terroristi e criminalità organizzata che sfruttano i proventi degli attacchi per finanziarsi*

- *il 6% ritiene che il pericolo si annidi all'interno dell'azienda, mentre il 25% sospetta che tali frodi possano essere realizzate da qualcuno esterno all'organizzazione con la complicità dei dipendenti*

- *il 42% delle imprese ha al proprio interno uno specialista capace di fronteggiare eventuali attacchi informatici*

- *il 20% ha preferito delegare ad una società esterna la funzione IT security*

- ***il 53% delle aziende ha messo in atto un piano o ha scelto di tutelarsi con delle polizze assicurative per difendersi dagli attacchi informatici***

Iniziativa proattiva delle Aziende / Persone fisiche

Come si protegge la Reputazione Aziendale da Cyber crime?

La gestione del rischio reputazionale deve basarsi essenzialmente:

a) sul **monitoraggio continuo del valore della propria reputazione**

b) sulla **consapevolezza di tale problematica a livello del management**

ERGO:

1) PREVENZIONE

2) TRASFERIMENTO DEL RISCHIO DI DANNO REPUTAZIONALE ALLE COMPAGNIE DI ASSICURAZIONE (?)

Quali possono essere i rischi da ipotizzarsi in copertura per il Danno Reputazionale Aziendale da Cyber crime?

1) Sottrazione di dati e documenti aziendali, diffusi all'esterno dell'azienda, con conseguente lesione della reputazione del titolare di dati (azienda ospedaliera, cartelle cliniche pazienti) → copertura assicurativa dell'azienda per il danno cagionato al terzo e conseguente risarcimento – processo e/o sanzioni a cui doversi opporre.

2) Azienda che opera commercialmente, ignara del crimine informatico che sta commettendo. Responsabilità anche penale ex L. 231/2001 dell'Amministratore delegato → copertura assicurativa del dirigente e dell'azienda (risarcimento danno a terzi e condanna pecuniaria ex L 231/2001).

3) Sottrazione di dati da parte di un dipendente di un'azienda concorrente e conseguente lesione della reputazione del terzo → responsabilità della società assicurata e richiesta di risarcimento dei danni subiti dal terzo.

4) Azienda concorrente che copia i prodotti dell'azienda assicurata, cagionando danni alla reputazione di quest'ultima → copertura assicurativa dei costi del procedimento d'urgenza volto ad interdire il protrarsi dell'utilizzo dei dati e delle informazioni relative ai prodotti copiati, oltre ad impedire l'aggravamento del danno reputazionale dell'azienda assicurata.

Opportunità per il mercato assicurativo

RISCHIO CYBER SEMPRE IN AUMENTO
(aumento della domanda sul mercato)

→ **CONSAPEVOLEZZA DEL RISCHIO?**

→ **OFFERTA ASSICURATIVA SPECIFICA?**

CONOSCERE BENE

CONOSCERE PRIMA

⇔

MAGGIORE TUTELA E SICUREZZA

MENO COSTI

↓

Consulenza preventiva

Grazie per l'attenzione!

Mario Dusi
Avvocato in Milano e Monaco di Baviera

DusiLaw Legal&Tax, Milano – Via Fontana 19, Tel. +39 02 55188121
www.dusilaw.eu