Regolamento UE 2016/679 (GDPR)
e
Cybersecurity

Avv. Ivan Rotunno
Orrick, Herrington & Sutcliffe LLP
irotunno@orrick.com

Contenuti

1. Entrata in vigore e ambito di applicazione
2. Impianto sanzionatorio
3. Le principali novità
4. Sicurezza e Data Breach
5. GDPR Roadmap
6. Cybersecurity

1. Entrata in vigore e ambito di applicazione

Regolamento UE 679/2016

Entrata in vigore

A partire dal **4 maggio 2016**, con la relativa pubblicazione sulla Gazzetta Ufficiale dell'Unione Europea (GUUE), il nuovo impianto normativo del cd. «*Pacchetto protezione dati UE*» si compone dei seguenti provvedimenti:

- **Regolamento**, avente a oggetto la *"tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati"*, e che disciplina i trattamenti di dati personali, sia nel settore privato, sia nel settore pubblico, e destinato ad abrogare la Direttiva 95/46/CE; e
- **Direttiva**, che detta una *"regolamentazione dei settori di prevenzione, contrasto e repressione dei crimini, nonché all'esecuzione delle sanzioni penali"*, e verte principalmente sulla protezione dei dati personali scambiati dalle autorità di polizia e giustizia.

La Direttiva è entrata in vigore il **5 maggio 2016** e dovrà essere recepita dagli stati membri entro **2 anni** mediante adeguamento degli ordinamenti interni.

Entrata in vigore del Regolamento

4 maggio 2016

Pubblicazione del Regolamento nella Gazzetta Ufficiale dell'UE

25 maggio 2018

Applicabilità del Regolamento **in tutti i Paesi UE**

2016 | 2017 | 2018

25 maggio 2016

Entrata in vigore del Regolamento

Ambito di applicazione territoriale

Il Regolamento si applica pertanto al trattamento dei dati personali di persone fisiche

effettuato:

- da un **titolare** del trattamento **stabilito** nel territorio dell'Unione Europea;

- da un **titolare non stabilito** nel territorio dell'Unione Europea **SE** il trattamento riguarda dati di persone residenti nell'UE e, in particolare, l'offerta di beni e servizi a tali soggetti nonché il monitoraggio dei loro comportamenti nell'UE.

pertanto

Qualsiasi entità/organizzazione/azienda che operi nell'Unione Europea sarà soggetta al Regolamento, a prescindere dal luogo in cui risiede.

2. Impianto sanzionatorio

Regolamento UE 679/2016

Impianto sanzionatorio

Le sanzioni amministrative pecuniarie sono le seguenti:

- Fino a **10,000,000** di Euro o, per le imprese, il **2%** del fatturato mondiale totale annuo dell'esercizio precedente nel caso di **violazione di alcuni obblighi** posti dal Regolamento (a es. per la violazione delle previsioni in materia di privacy by design e by default).
- Fino a **20,000,000** di Euro o, per le imprese, il **4%** del fatturato mondiale totale annuo dell'esercizio precedente nel caso di **violazione di altri obblighi più stringenti** posti dal Regolamento (a es. per la violazione delle previsioni in materia di trattamento lecito corretto e trasparente dei dati, trattamento di dati particolari quali opinioni politiche, convinzioni religiose).

Con riferimento invece alla determinazione delle **sanzioni penali**, gli Stati Membri dovranno, entro il 25 maggio 2018, prevedere idonee sanzioni e informare la Commissione.

3. Le Principali Novità

Nuove figure e nuovi adempimenti

Regolamento UE 679/2016

orrick

Principali novità

Consenso: Libero, specifico, informato, inequivocabile e concludente.

Informativa: Informazioni di contatto titolare, rappresentante e responsabile protezione dei dati; indicazione della finalità di trattamento; destinatari e categorie di dati trattati; trasferimento dati personali in paesi terzi; diritti azionabili e implicazioni; ricorrenza di altre basi giuridiche diverse dal consenso.

Valutazione impatto: Ripensamento delle tecnologie a supporto dei trattamenti. Analisi e eventuale consultazione preventiva con l'Autorità Garante per le implicazioni sui diritti e le libertà delle persone.
Obbligo del titolare, supportato dal responsabile protezione dati.

Sicurezza: Analisi dei rischi e di valutazione dell'adeguatezza delle misure tecniche e organizzative.
Obbligo che grava congiuntamente su titolare e responsabile del trattamento dati.

Violazione dei dati: Equiparazione della fattispecie accidentale con quella dolosa.

Privacy by Design & Privacy by Default: Applicazione delle tutele di trattamento sin dalla sua progettazione e avvio. Pseudonimizzazione e Minimizzazione (di dati e tempi) come garanzia e misura di Privacy by Design.
Obbligo che grava sul titolare.

Data Protection Officer: Si interfaccia con le Autorità Garanti. Supporta titolare e responsabile del trattamento.
Obbligatorio in alcuni casi, la sua nomina grava sul Titolare e/o sul Responsabile.

Principali novità

Registro Trattamenti: Registri di competenze in cui indicare le caratteristiche, le modalità e le finalità del trattamento.
Lo redigono titolare e responsabile del trattamento.

Sanzioni: Sanzioni amministrative pecuniarie fino a 20 000 000 EUR (per le imprese, fino al 4% del fatturato globale annuo dell'esercizio precedente).

Autorità: Istituendo comitato di controllo europeo che assicura la uniforme applicazione del Regolamento. Autorità di Controllo: autorità pubblica indipendente di uno Stato membro.

Profilazione: L'interessato ha il diritto di non subire trattamenti automatizzati (profilazione) inconsapevoli.

Portabilità dei Dati: L'interessato ha il diritto ottenere la restituzione dei propri dati personali trasmessi e trattatati da un titolare e trasmetterli ad altri.

Oblio: L'interessato ha diritto alla de-indicizzazione o alla cancellazione delle informazioni che lo riguardano.

Sportello Unico: Unicità dell’interlocutore territoriale. Semplificazione e uniformità di gestione nell’applicazione del nuovo regolamento.

4. Sicurezza e *Data Breach*

Regolamento UE 679/2016

Sicurezza e *Data Breach*

Con riferimento al tema della **sicurezza nel trattamento** dei dati, l'articolo 5 del Regolamento prevede che il trattamento dei dati sia effettuato con modalità che garantiscano un'adeguata sicurezza e protezione anche mediante l'adozione e l'utilizzo di misure tecniche e organizzative adeguate.

Tra le misure di sicurezza individuate dall'articolo 32 del Regolamento vi sono, a titolo esemplificativo:

- la **cifratura** dei dati personali;
- il **mantenimento della riservatezza** e dell'integrità su base permanente;
- il **ripristino tempestivo**, se necessario, della disponibilità e dell'accesso dei dati in caso di incidente fisico o tecnico;
- una **procedura per la verifica**, costante, dell'efficacia delle misure di sicurezza adottate.

Sicurezza e *Data Breach*

In caso vi sia una **violazione dei dati**, tutti i titolari del trattamento devono tempestivamente – dove possibile entro e non oltre 72 ore dal momento in cui ne sono venuti a conoscenza – notificare l'avvenuta violazione al *Garante Privacy*.

Tale **notifica deve contenere**, tra le altre cose, una descrizione della natura della violazione, il contatto del responsabile della protezione dei dati, le probabili conseguenze della violazione, le misure adottate e/o adottande.

La violazione deve essere notificata anche all'interessato qualora presenti un **rischio elevato** per i diritti e/o le libertà della persona fisica.

5. GDPR Roadmap

GDPR Roadmap

Fase 1. Assessment

L’attività di valutazione e revisione dei presidi già posti in essere dalla Società sarà compiuta mediante l’espletamento di un eterogeneo insieme di attività, tra cui si indicano, seppur non esaustivamente, le seguenti:

(i) ruoli e funzioni ascrivibili all’organigramma privacy;

(ii) procedure, informative sulla privacy e politiche aziendali già diffuse all’interno della Società;

(iii) politiche e/o accordi per il trattamento e il trasferimento dei dati personali verso giurisdizioni extra Unione Europea;

(iv) verifica della coerenza della nomina a responsabili esterni nei confronti dei fornitori/controparti contrattuali;

(v) svolgimento di interviste a figure che svolgono ruoli chiave per quanto riguarda il trattamento dei dati personali.

GDPR Roadmap

Fase 2. Gap Analysis

L'attività di *Gap Analysis*, volta all'analisi dei risultati emersi dalla precedente attività di *Assessment* e all'identificazione delle probabili e possibili soluzioni alle eventuali problematiche riscontrate, sarà espletata come segue:

- redazione di un report di sintesi che identifichi eventuali *gap* riscontrati e le attività che la Società dovrà intraprendere per garantire la conformità al GDPR;
- discussione del report con i rappresentanti a ciò preposti dalla Società.

GDPR Roadmap

Fase 3. Definizione e pianificazione degli interventi di adeguamento

Sempre sulla base del rapporto di *Gap Analysis,* si provvederà a tracciare una *roadmap* per la definizione del Piano operativo e temporale degli interventi per il raggiungimento della conformità alle prescrizioni del GDPR.

In particolare, la redazione della *roadmap* sarà effettuata sulla base del seguente approccio metodologico:

- Definizione elenco di interventi necessari associati ai rischi che si intende contrastare, sulla base della *gap analysis*: sintesi delle attività di miglioramento ed analisi delle sinergie possibili;
- Prioritizzazione in un'ottica *risk driven* dei progetti e delle attività;
- Indicazione tecnica delle misure di dettaglio da prevedere all'interno degli interventi;
- Definizione di massima di tempi ed *effort* degli interventi.

GDPR Roadmap

Fase 4. Assistenza all'implementazione degli interventi di adeguamento

Con l'obiettivo di realizzare gli interventi previsti dalla *roadmap*, dovranno esser svolte le seguenti attività:

- Integrazione dei processi e delle procedure aziendali non conformi al Regolamento;
- Predisposizione dei processi e delle procedure mancanti;
- Adeguamento dei sistemi informativi;
- Integrazione/modifica delle clausole contrattuali standard rispetto agli adempimenti richiesti dal GDPR e previsione di eventuali clausole *ad hoc* per contratti con particolare criticità in relazione al trattamento dei dati;
- Predisposizione del Registro dei Trattamenti.

6. Il Rischio Cybersecurity

6.1 Perché parliamo di Cybersecurity – Understanding the risk

Understanding the Risk

«Total cybersecurity is an unrealistic goal»

NACD – National Association of Corporate Directors, Cyber-Risk Oversight, 2017

Understanding the Risk – In Italia

In Italia, il **Rapporto 2015 dell'Associazione Italiana per la Sicurezza Informatica (Clusit)** ha quantificato i danni provocati dal *cybercrime* in un valore pari a nove miliardi di euro.

Il **Rapporto Clusit 2017**, invece, ha evidenziato che il 2016 è stato l'anno peggiore di sempre in relazione agli attacchi cyber; infatti, rispetto al 2015 sono cresciuti gli attacchi:

- al settore sanitario del 102%;
- alla grande distribuzione organizzata del 70%;
- al sistema finanziario del 64%.

Understanding the Risk – Una possibile definizione

Banca d'Italia nella Circolare n. 285/2013

«**Rischio informatico (o ICT)**»: ***il rischio di incorrere in perdite economiche, di reputazione e di quote di mercato in relazione all'utilizzo di tecnologia dell'informazione e della comunicazione (Information and Communication Technology – ICT).***

Understanding the Risk – Conseguenze economiche

Nell’ambito dell’impatto sui possibili investitori, un sondaggio pubblicato nell’aprile 2015 da KPMG ha riportato gli orientamenti di **oltre 130 investitori istituzionali** con operatività globale e asset in gestione per oltre tremila miliardi di dollari.

All’esito di questo sondaggio è risultato che **circa l’80%** dei soggetti intervistati ha dichiarato che avrebbe **evitato di investire o avrebbe posticipato la decisione di farlo in aziende che fossero state oggetto di attacchi informatici oppure prive di una comprovata strategia di sicurezza**.

Understanding the Risk – Conseguenze economiche

Secondo recenti stime (Lloyd's, 2015), a livello mondiale, i **cyber attack** oggi **costano alle aziende** circa **400 miliardi di dollari** e secondo stime del World Economic Forum il costo è stimato raggiungere la cifra di **3.000 miliardi nel 2020**.

Nel 2015 la società americana di ricerca Gartner ha evidenziato che la spesa globale per i prodotti e i servizi di sicurezza informatica rispetto al 2014 è cresciuta del 4,7%, toccando i 75 miliardi di dollari, e ha previsto – come riportato anche dalle società di ricerca Markets and Markets e Ssp Blue – una **spesa pari a 170 miliardi di dollari per il 2020**.

(Rivista Internal Audit 2016)

Understanding the Risk – Conseguenze economiche

Quindi il *cyber-risk* è una tipologia di rischio di impresa con un potenziale impatto economico rilevante in quanto può comportare:

- *danni reputazionali;*
- *perdite di proprietà intellettuale;*
- *furto di denaro*;
- *perdita di informazione strategiche* per la conduzione del business;
- *costi* per il *ripristino dell'operatività* o per far fronte ai *danni subiti*;
- *rischio da mancato investimento*;
- *spese legali*.

6. Il Rischio Cybersecurity

6.2 Evoluzione della condotta rilevante - Il Cyber-crime

Il Cybercrime - Definizione

- Nel trattato del **Consiglio d'Europa** sulla criminalità informatica viene utilizzato il termine «**cybercrime**» per definire reati che vanno dai **crimini contro i dati riservati**, alla **violazione di contenuti** e del **diritto d'autore**.

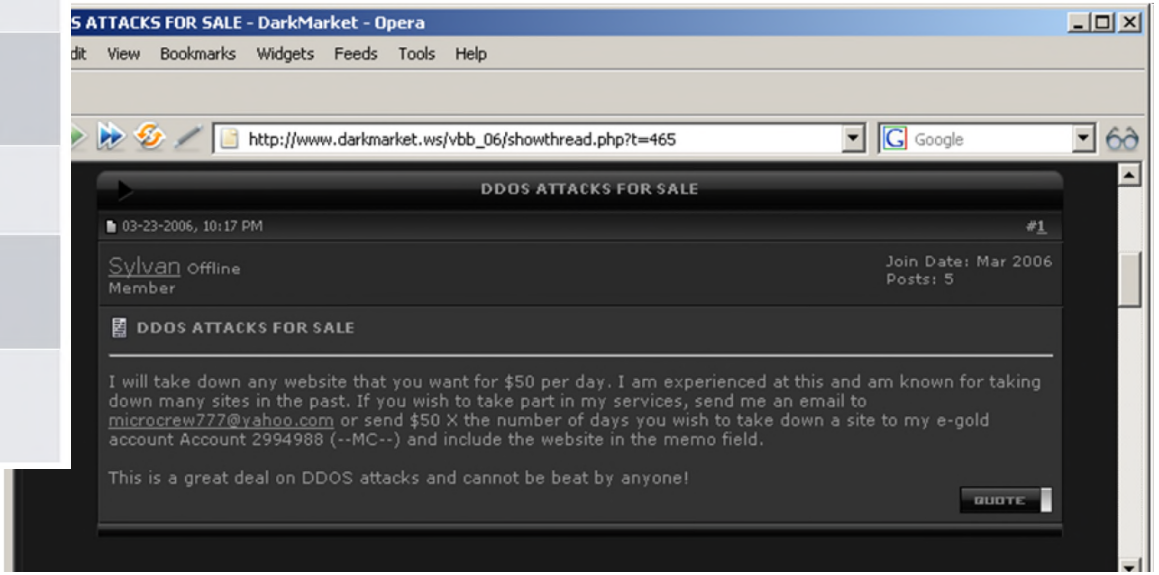
- Il manuale delle Nazioni Unite sulla prevenzione e il controllo del crimine informatico (***The United Nations Manual on the Prevention and Control of Computer Related Crime***) nella definizione di crimine informatico include **frode, contraffazione e accesso non autorizzato** [Nazioni Unite, 1995].

Il Cybercrime – Condotte

Service Name	Service Pricing (USD)
Xakepy.cc	1 hour starts at $5 24 hr starts at $30 1 week starts at $200 1 month starts at $800
World DDoS Service	1 day starts at $50 1 week starts at $300 1 month starts at $1,900
King's DDoS Service	1 hour starts at $5 12 hours starts at $25 24 hours starts at $500 1 month starts at $1,500
MAD DDoS Service	1 night starts at $35 1 week starts at $180 1 month starts at $500
Gwaspo's Professional DDoS Service	1-4 hours at $2/hr 5-24 hrs at $4/hr 24-72 hrs at $5/hr 1 month at $1,000 fixed
PayCho DDoS Service	1 hour for $6 1 night for $60 1 week for $380 1 month for $900

Attacchi Dos/DDoS
Denial of Service/ Distributed Denial of a Service

indica un malfunzionamento dovuto ad un attacco informatico in cui si fanno esaurire deliberatamente le risorse di un sistema informativo che fornisce un servizio ai client, ad esempio un sito web su un web server, fino a renderlo non più in grado di erogare il servizio ai client richiedenti



Il Cybercrime – Condotte

- Hackeraggio dei server aziendali dall'esterno
- Attacchi riusciti di phishing
- Credenziali di accesso annotate su un post-it dimenticato in treno o in taxi
- Informazioni personali inviate al destinatario sbagliato
- Laptop o dispositivo di memoria dimenticato o lasciato nel posto sbagliato (es.: il trasportatore lo perde)
- Pubblicazione non voluta di informazioni personali su un sito internet pubblico
- Modalità improprie di utilizzo e gestione di back-up o copie cartacee
- Furto di dati o di dispositivi di memoria da parte di dipendenti e/o terze parti

Minacce (1/2)

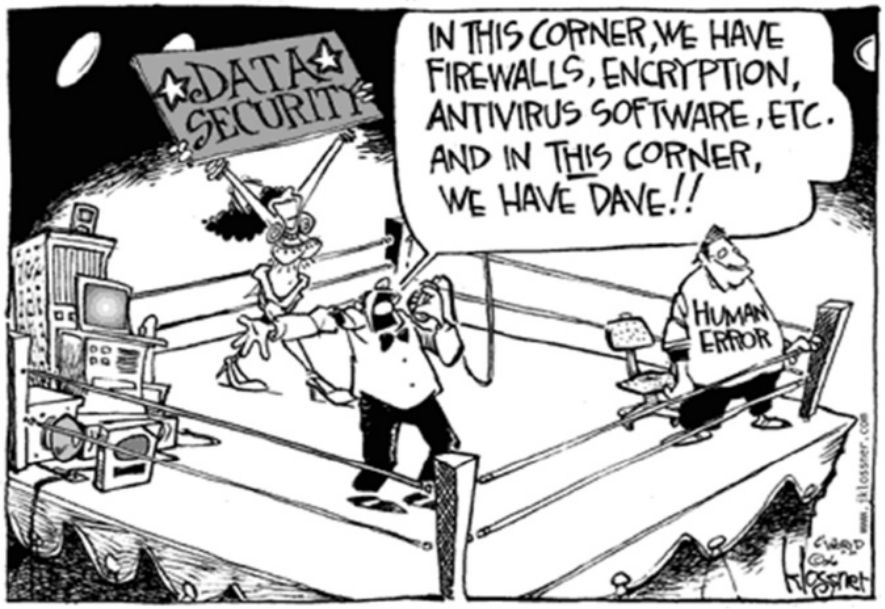
Tipologie di Attori vs. Tipologie di Impatti

IMPATTI / ATTORI	Furti / Frodi Finanziarie	Furto di proprietà intellettuale nei piani strategici	Interruzione del business	Distruzione di infrastrutture critiche	Danno reputazionale	Minacce alla Safety / Life	Regolatorio
Criminalità organizzata	Molto Alto	Moderato	Basso	Basso	Molto Alto	Basso	Molto Alto
Hacktivist	Alto	Moderato	Molto Alto	Alto	Molto Alto	Basso	Alto
Stati – Nazioni	Alto	Alto	Molto Alto	Molto Alto	Molto Alto	Basso	Molto Alto
Insider	Molto Alto	Alto	Alto	Alto	Alto	Moderato	Alto
Terze parti	Alto	Moderato	Moderato	Moderato	Molto Alto	Basso	Molto Alto
Hacker Singoli	Molto Alto	Alto	Alto	Alto	Alto	Basso	Alto

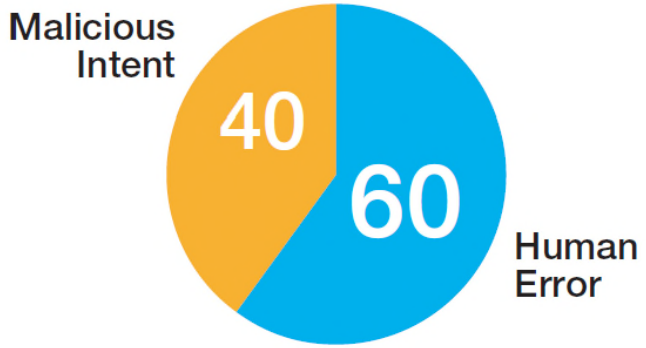
Molto Alto Alto Moderato Basso

Fonte: Deloitte Center for Financial Services, "2015 Banking Outlook Boosting profitability amidst new challenges"

Minacce (2/2)



Errore o dolo?



Attraverso lo schema della **Business Email Compromise (BEC)** secondo le stime Verizon nel **2015** sono stati erronemente pagati **circa $110Mio** dalle aziende americane a fronte di frodi via e-mail

Il Cybercrime – Obiettivi

La compromissione delle strutture informatiche può concretizzarsi in attacchi su vasta scala o azioni mirate e avere motivazioni politiche o, più spesso, volte ad acquisire vantaggi economici:

- ***Rubare informazioni***
- ***Rubare soldi***
- ***Effettuare estorsioni***
- ***Ricattare***
- ***Trafugare segreti industriali e commerciali***

6. Il Rischio Cybersecurity

6.3. Considerazioni conclusive

I metodi di approccio al cyber risk

- Il rischio *cyber* **non** può essere trattato secondo i canoni tradizionali che lo vincolano al **solo perimetro di infrastrutture ICT.**
- L'approccio adeguato richiede una **visione completa di tutte le relazioni che intercorrono tra i processi, le informazioni aziendali e i servizi accessibili attraverso il cyberspazio**.
- Dati gli impatti e le conseguenze che il *cybercrime* può comportare per un'impresa le soluzioni operative devono essere ricercate nella ***collaborazione di tutte le funzioni coinvolte (IT, legale, risorse umane, operations, organizzazione) al fine di costruire un sistema efficace i cui ruoli non sono facilmente separabili***.
- La complessità della materia richiede che il ***cyber risk* management** debba fondarsi sulla multidisciplinarietà costituendo, quindi, prima di tutto un tema **attinente alla governance societaria**.

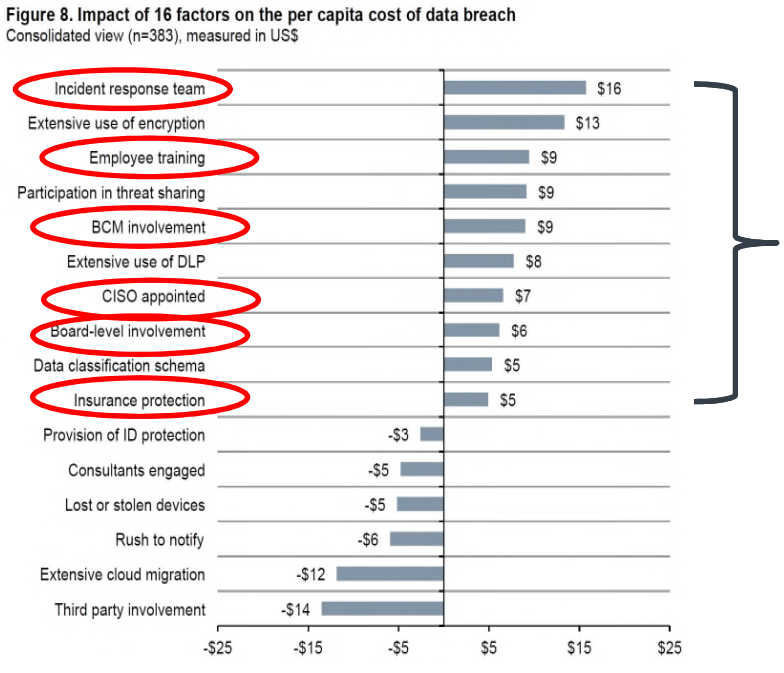
Il Cyber Risk come problema di Governance

Alla luce di quanto sopra, si deve concludere che il ***cyber-risk*** è, prima di tutto, un **problema di governance**.

I metodi di approccio al cyber risk

Il corretto approccio dovrebbe coinvolgere, da un lato, un ***team multidisciplinare*** e, dall'altro, un'analisi trasversale delle attività critiche per la sicurezza informatica di ogni processo aziendale (***IT, organizzazione, gestione delle risorse umane, ciclo degli acquisti, affari legali, comunicazione e funzioni aziendali di controllo interno***).

I metodi di approccio al cyber risk



Source: Ponemon Institute/IBM, 2016 Cost of Data Breach Study, Global Analysis

Il corretto approccio consente anche di ridurre i costi di ogni singolo attacco.

In questo studio IBM, viene dimostrato come l'esistenza di presidi quali un incident response team, l'uso di sistemi di encryption, la formazione dei dipendenti, la nomina di un CISO (Chief Information Security Officer) e la business continuity diminuiscano i costi di ogni singolo attacco.

Ad esempio, secondo questo studio, la presenza di un incident response team reduce il costo di un singolo attacco di $ 16, da $158 a $142 mentre il coinvolgimento di soggetti terzi provoca un aumento dei costi di $14 per attacco, da $158 a $172.

I metodi di approccio al cyber risk

Nell’ambito dell’analisi del rischio bisogna tenere in considerazione che, in base allo studio elaborato dalla AFCEA Cyber Committee, The economics of cybersecurity, 2014, questi **controlli base sono efficaci nel prevenire l’85% delle cyber-intrusioni** e potenzialmente in grado di ridurre l’impatto economico dei cyber-attack:

1. Restringere la **facoltà di installazione di applications** da parte degli user;
2. Assicurarsi che i **sistemi operativi e i software siano sempre aggiornati** con le ultime release prima verificate dalle funzioni ITC interne;
3. Restringere i **privilegi di administrator**.

Avv. Ivan Rotunno

Orrick, Herrington & Sutcliffe LLP

irotunno@orrick.com