Il 49% dei data breach provocati da un errore umano

Lug 25, 2019 Marco Schiaffino Attacchi, Gestione dati, Hacking, In evidenza, Leaks, Malware, News, RSS, Scenario 0

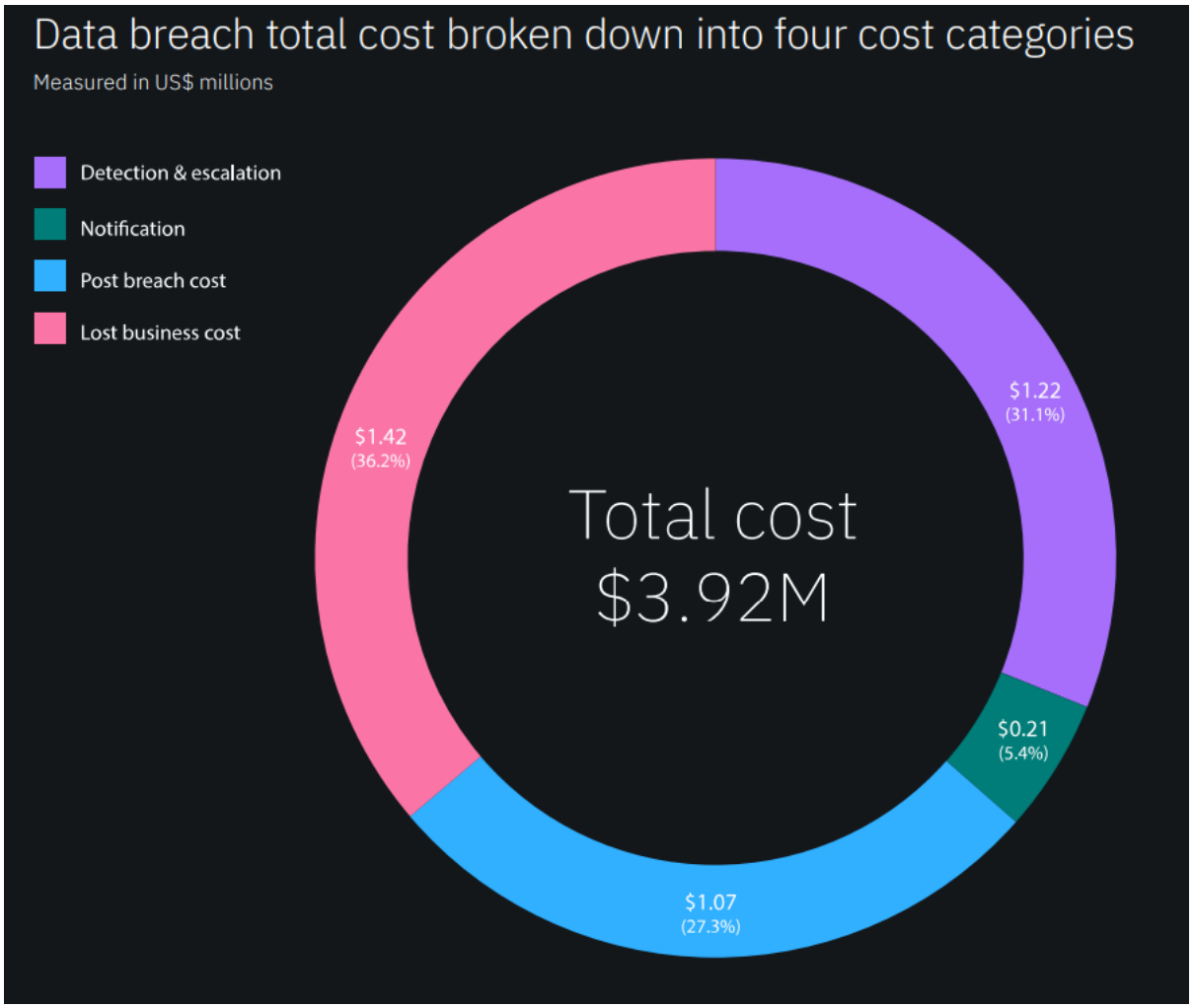
La ricerca è stata condotta di IBM e Ponemon Institute. Aumentano i costi per rimediare alle violazioni e le piccole aziende spendono di più di quelle grandi.

Per inquadrare una situazione, spesso, è più utile qualche numero che migliaia di parole. Da questo punto di vista, il report intitolato **Cost of a Data Breach** pubblicato da **IBM** in collaborazione con il **Ponemon** Institute è un esempio cristallino (e preoccupante) in termini di chiarezza.

Lo studio, che si può scaricare attraverso una procedura di registrazione da questo sito, si basa su un campione di 507 aziende e interviste sottoposte a 3.211 persone. I dati che emergono riescono a quantificare un fenomeno sul quale la sensibilità sta crescendo, anche se troppo lentamente.

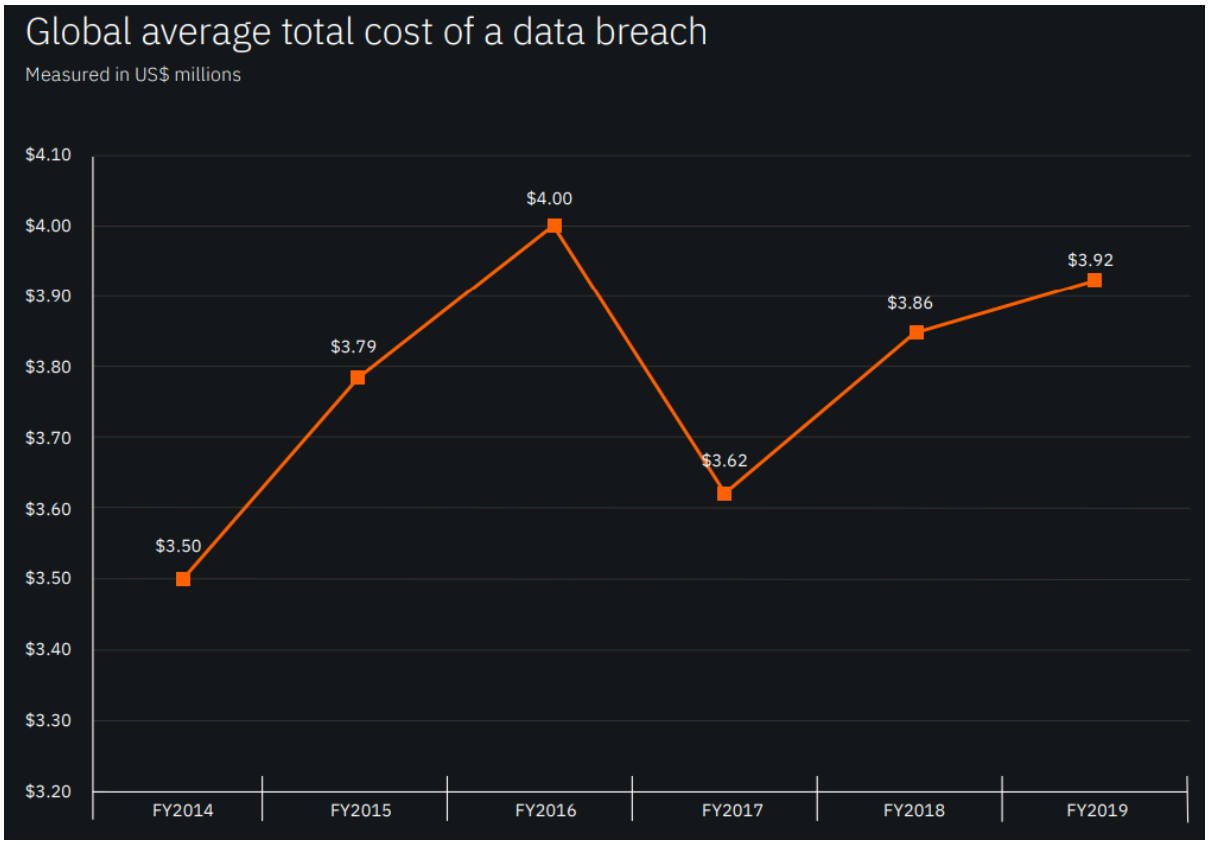
Anche perché, secondo la ricerca, il costo medio per il recupero da un data breach non è esattamente a buon mercato: ammonterebbe infatti a **3,92 milioni di dollari**, con un costo medio di 150 dollari per record.

Una valutazione che i ricercatori spiegano con il fatto che le conseguenze di un data breach si dispiegano in realtà per un lungo periodo di tempo. A incidere in maniera determinante sul danno è la perdita in termini di business, che lo studio quantifica nel 36% del costo totale.



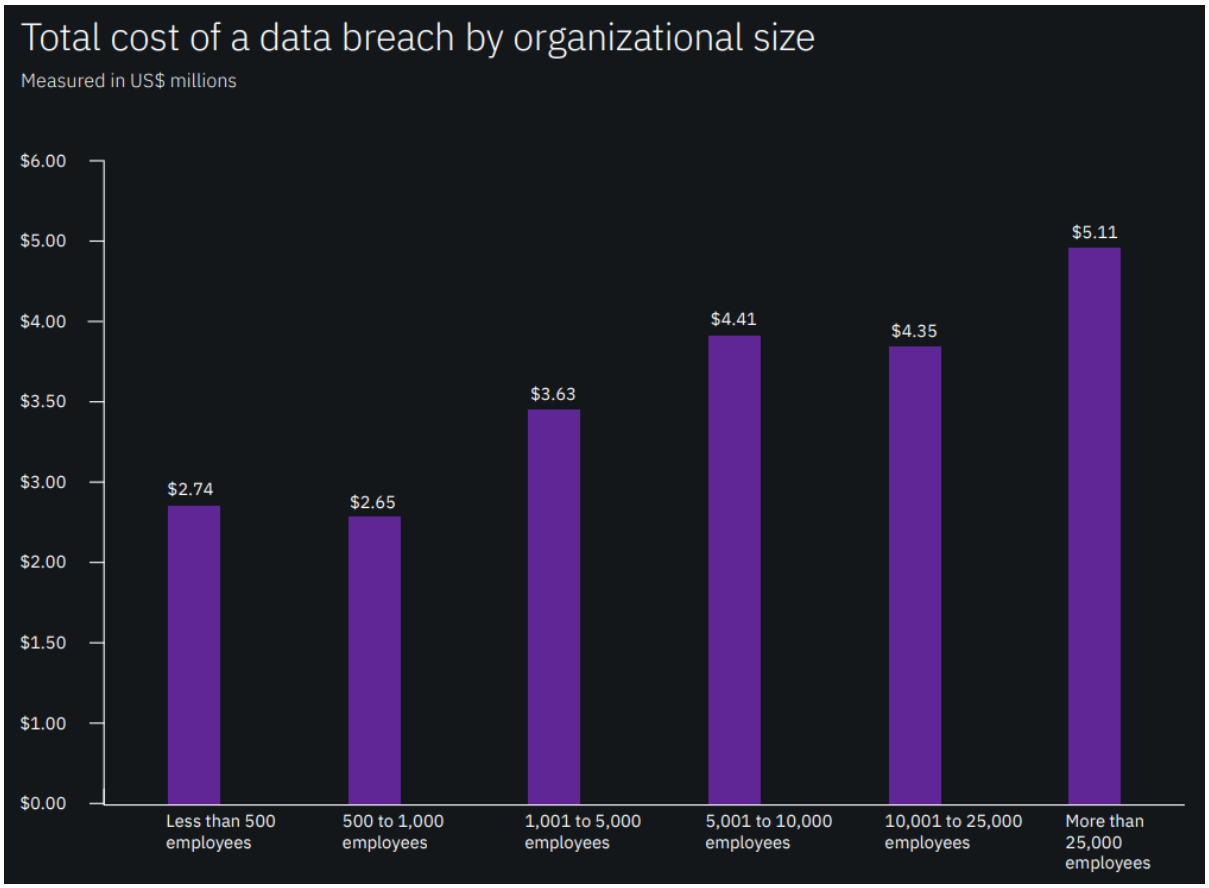
Il concetto di “tempi lunghi” riguarda anche un altro aspetto, quello della scoperta e reazione al data breach. In media si parla di **279 giorni** (9 mesi!) necessari per individuare il problema e risolverlo.

Cambiando la prospettiva, emerge come gli attacchi dei pirati informatici rimangano la causa più rilevante delle violazioni di dati. **Non solo: sono anche quelli che provocano maggiori danni (4,45 milioni di dollari) sotto il profilo dei danni e dei costi di ricovero**.

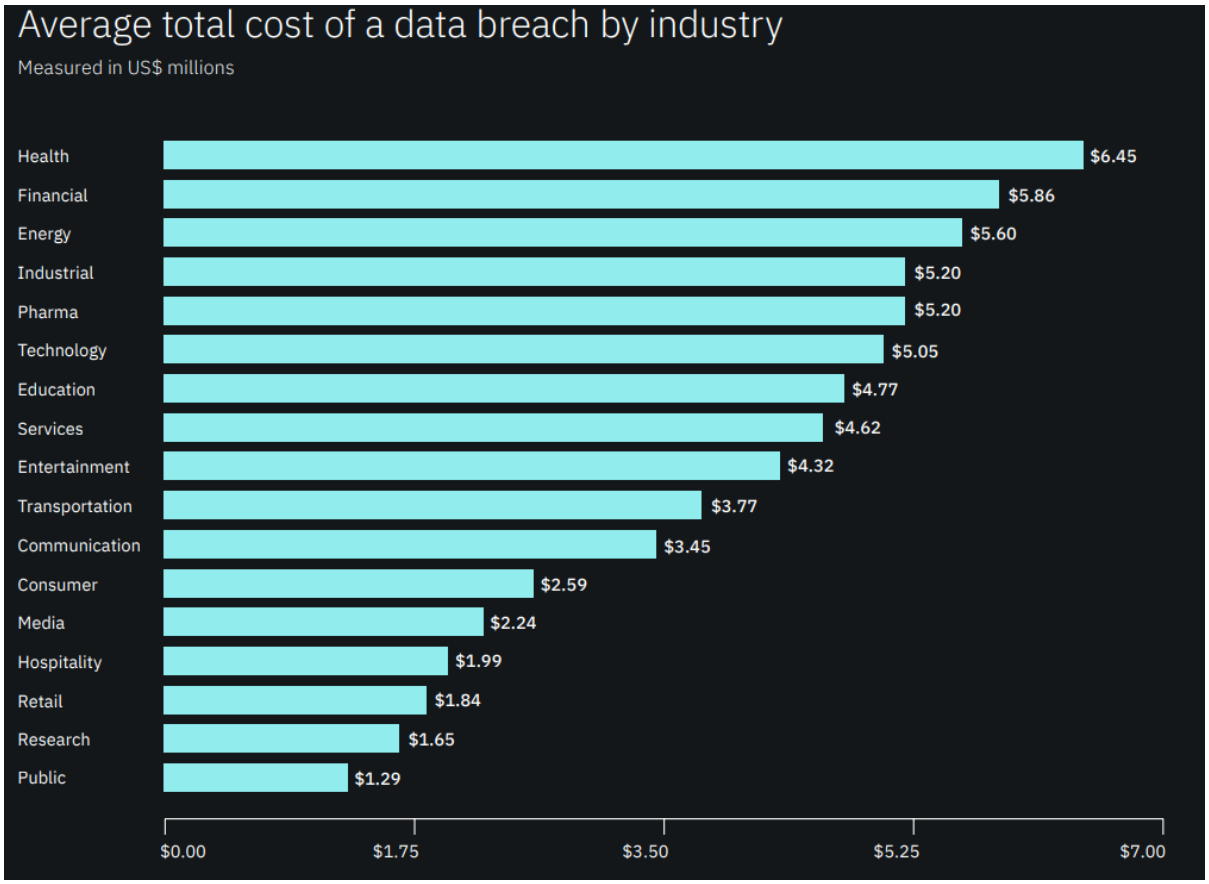


Il dato impressionante, però, riguarda il numero di breach provocati da semplici errori umani, come errate configurazioni ed esposizione involontaria dei dati. **Stiamo parlando del 49% dei casi studiati nel rapporto**. Per contro, questo tipo di incidenti hanno un costo inferiore per le aziende rispetto a quelli provocati dagli attacchi dei cyber-criminali. **Il costo medio varia tra i 3,24 e i 3,5 milioni di dollari**.

Un altro dato interessante riguarda l'impatto in termini di costi a seconda delle dimensioni della aziende. Quelle più grandi (più di 25.000 dipendenti) subiscono un danno medio di 5 milioni di dollari, cioè 200 dollari circa per impiegato.



Le imprese di dimensioni medie (tra 500 e 1.000 dipendenti) si collocano su una media di 2,65 milioni di dollari: **3.533 dollari per impiegato**. La differenza riguarderebbe un classico fenomeno di economia di scala, per cui le aziende più grandi riuscirebbero ad arginare con maggiore facilità il danno economico.



Per quanto riguarda invece il settore di attività, quello che subisce i maggiori danni è quello relativo alla sanità, seguito dai servizi finanziari, dal settore energetico e da quello industriale.

Insomma: se incontrate qualcuno che si ostina a dare scarsa importanza al tema della cyber-security, speditegli il link della ricerca IBM. Il risultato è assicurato.

Condividi l’articolo

Una nuova immagine, una nuova identità, una nuova visione del futuro: Earth 2050! C’è una falla in VLC? Sì, no, forse…

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/07/25/il-49-dei-data-breach-provocati-da-un-errore-umano/