LA RICERCA VENUTA DAL FUTURO
1923 CNR 2023

Caratterizzazione del cyber-risk attraverso l'analisi di database pubblici di incidenti informatici

M.F. Carfora e A. Orlando
IAC - CNR

Istituto per le Applicazioni del Calcolo "Mauro Picone"

Consiglio Nazionale delle Ricerche

Il Centenario del CNR è realizzato con il contributo della Presidenza del Consiglio dei Ministri e con il Patrocinio di Rai

PRESIDENZA DEL CONSIGLIO DEI MINISTRI
Struttura di missione anniversari nazionali ed eventi sportivi nazionali e internazionali

ANNIVERSARI NAZIONALI

Rai

Categorie di rischio

Finanziari

Strategici

Compliance

Operativi

Cyber Risk

Cyber risk come rischio operativo

Per rischio operativo si intende il **rischio di perdite derivanti dall'inadeguatezza o dalla disfunzione di procedure, risorse umane e sistemi interni, oppure da eventi esogeni.**

L'Institute of Risk Management definisce il **rischio cyber** come il rischio di incorrere in perdite finanziarie in seguito al verificarsi di eventi accidentali o di azioni dolose inerenti il sistema informatico.

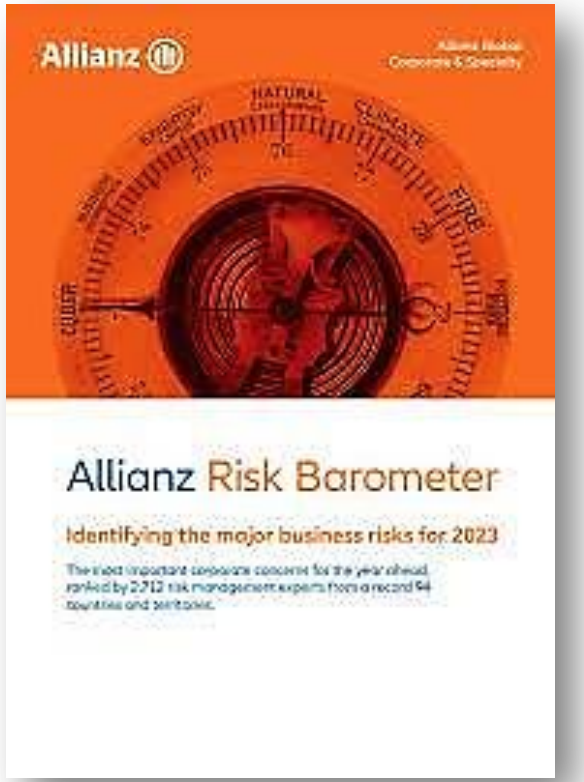
Il rischio cyber può avere caratteristiche sistemiche: casi isolati possono ripercuotersi su scala ben maggiore.

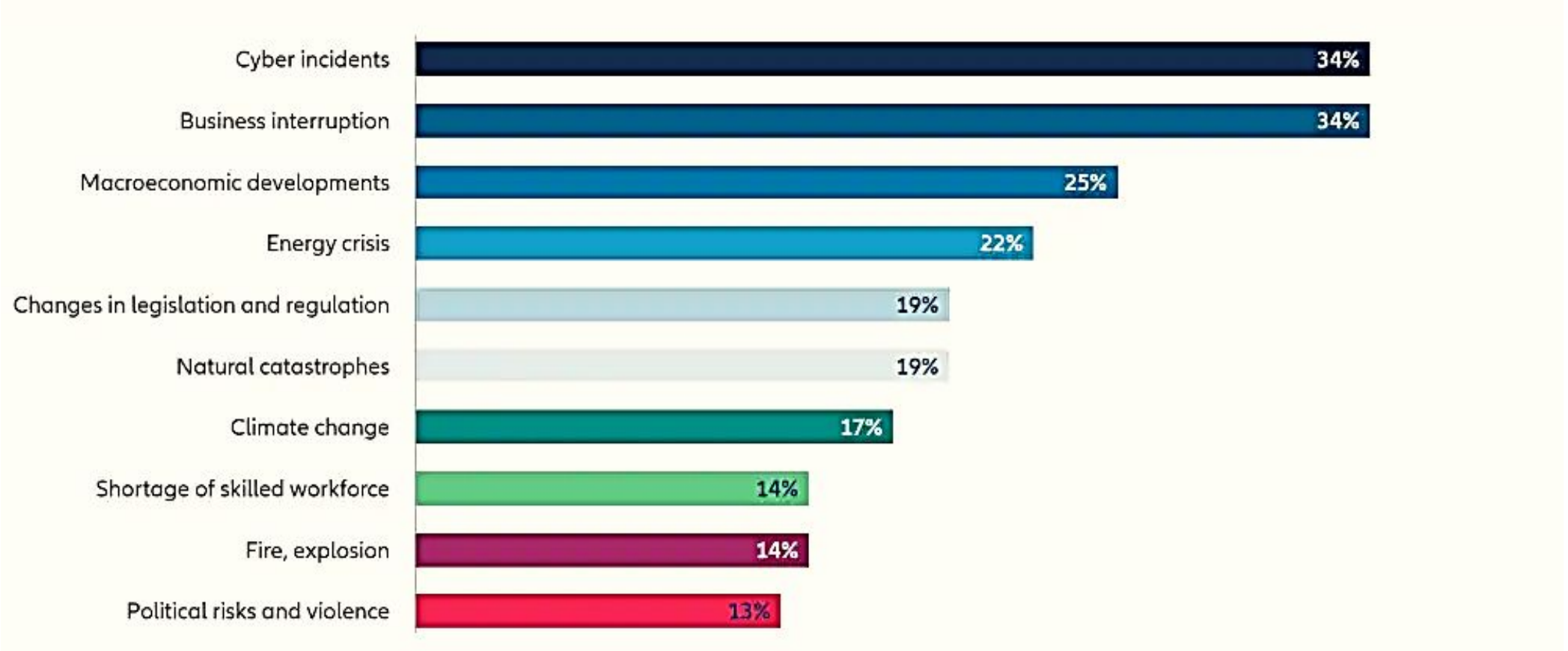
Allianz Risk Barometer 2023

L'indagine annuale sui rischi aziendali globali di Allianz Global Corporate & Specialty (AGCS) incorpora le opinioni di un campione statisticamente significativo di esperti in 92 paesi, inclusi amministratori delegati, gestori del rischio, broker ed esperti assicurativi.

In base al rapporto **del 2023 i rischi informatici affiancano quello da interruzione di attività in cima alla classifica dei rischi più temuti dalle aziende di tutto il mondo**.

La criminalità informatica costa 1trn di dollari all'anno, circa l'1% del PIL mondiale.

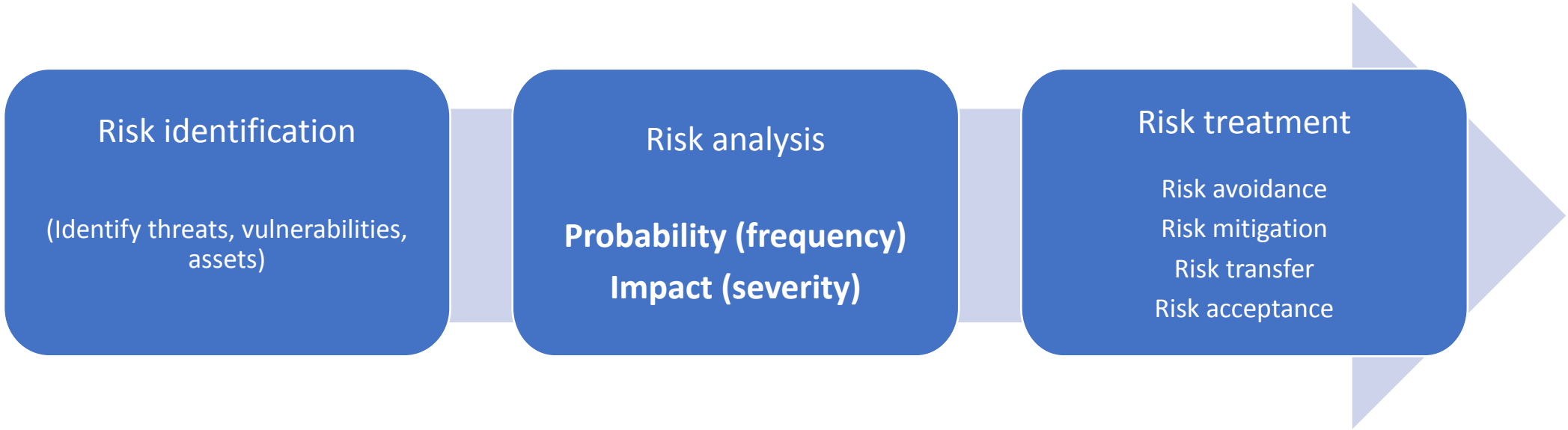



Cyber incidents
34%
Business interruption
34%
Macroeconomic developments
25%
Energy crisis
22%
Changes in legislation and regulation
19%
Natural catastrophes
19%
Climate change
17%
Shortage of skilled workforce
14%
Fire, explosion
14%
Political risks and violence
13%

Danni potenziali

- danni da **interruzione di attività**;
- danni **materiali** ai sistemi elettronici e informatici;
- richieste di **risarcimento** danni da parte di terzi;
- **danno reputazionale** e perdita di clienti e fornitori;
- costi emergenti per **servizi professionali**.

Gestione del rischio



Mitigazione e trasferimento del rischio informatico

Self-protection

Self-insurance

complementari

sostituti

Cyber insurance

Trasferimento del «rischio residuo» ad una compagnia di assicurazione

Criticità dell’assicurazione cyber

- continua evoluzione dei sistemi informatici
- attacchi informatici sempre più sofisticati e frequenti
- interdipendenza fra i livelli di sicurezza delle aziende
- l’impatto è difficile da determinare
- asimmetria informativa
- carenza di dati

Calcolo dei premi assicurativi

Supponiamo che una compagnia di assicurazione debba risarcire la perdita finanziaria in riferimento ad un periodo pari ad un anno.

- N numero casuale di incidenti informatici che si verificano durante l'anno di copertura assicurativa
- L_k la perdita finanziaria causata dal k-esimo incidente, k=1,2,3,...,N.

Si ipotizza che le perdite aleatorie L_k , k=1,2,3,...,N siano mutuamente indipendenti, abbiano la stessa distribuzione di probabilità e siano indipendenti dalla frequenza degli incidenti.

L'assicuratore deve quantificare il risarcimento Y_k relativo alla perdita k-esima.

In caso di copertura parziale $Y_k < L_k$ mentre in caso di risarcimento pieno $Y_k = L_k$.

Il costo complessivo X per la compagnia di assicurazione, in riferimento al periodo di copertura, è pari a

$$X = 0, \text{ se } N=0 \quad \text{e} \quad X = Y_1 + Y_2 + Y_3 + \ldots + Y_N, \text{ se } N>0$$

Calcolo dei premi assicurativi

L'assicuratore calcola il cosiddetto *Equivalence Premium* Π ovvero quella quantità tale che risulti Π=E[X].
A questa somma aggiungerà un caricamento di sicurezza che può essere calcolato in base a diversi criteri indicati dalla letteratura.

Di seguito alcuni semplici esempi:

Expected value principle: $P_{ev} = (1+\alpha)\,\Pi$

Variance principle: $P_{var} = \Pi + \alpha\sigma_X^2$

Standard deviation principle: $P_{var} = \Pi + \alpha\sigma_X$

Value at risk

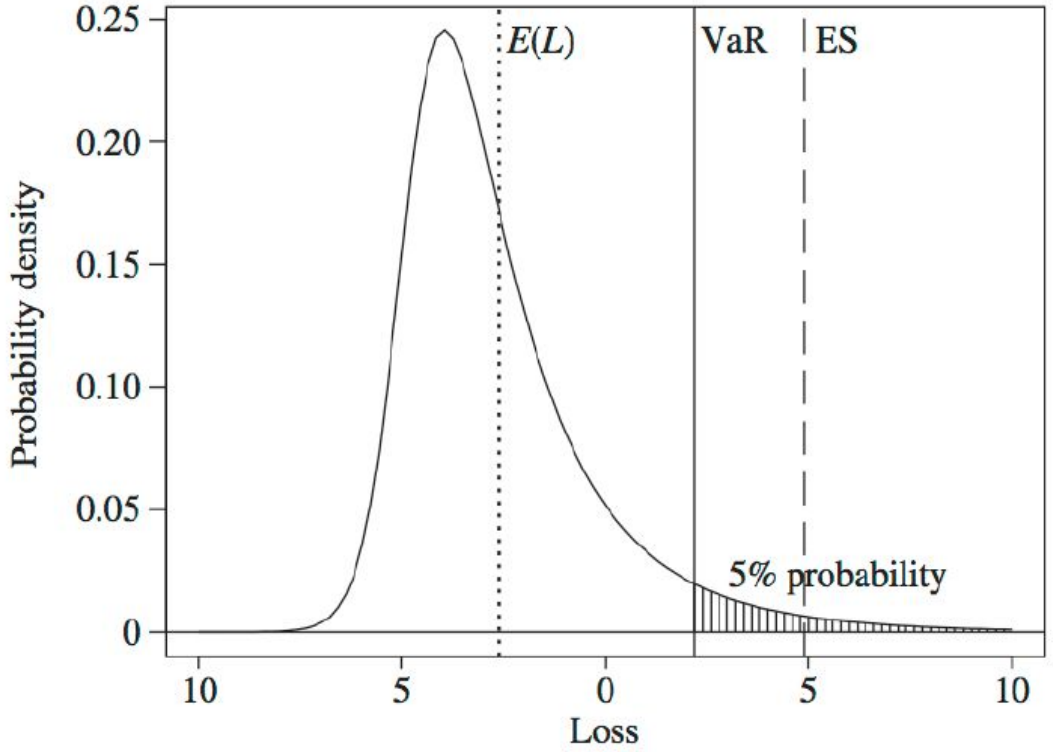
Un'informazione molto importante, sia per l'assicuratore che per l'assicurato, riguarda la stima delle perdite dovute agli eventi estremi. A tal fine, nella letteratura relativa alla quantificazione del rischio cyber, si fa riferimento anche ad indicatori solitamente utilizzati in ambito finanziario.

Il VaR (Value at Risk), fissato un livello di confidenza (1-α) con $\alpha \in [0,1]$, è la massima perdita potenziale calcolata su un dato orizzonte temporale

$$VaR_\alpha = inf[l \in R | P(L < l) \leq (1-\alpha)]$$

Una misura di rischio che fornisce informazioni circa le perdite superiori al VaR è il Tail VaR o Expected Shortfall:

$$TVaR_\alpha(L) = E[L | L \geq VaR_\alpha]$$



Fonte: Embrechts et al., Quantitative Risk Management (ed. 2015)

Modellare il rischio cyber

Descrivere il rischio significa costruire un modello che permetta di:

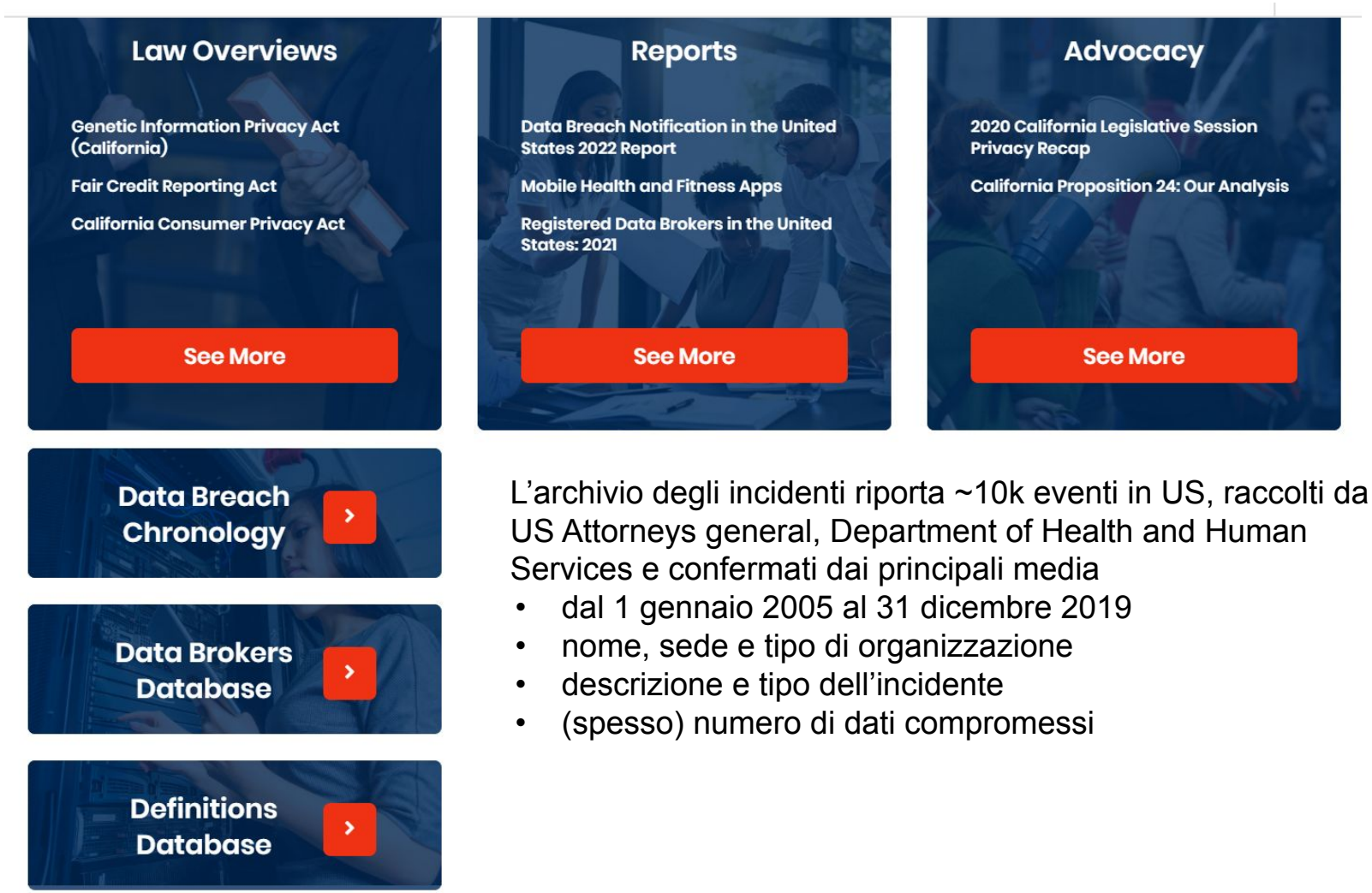
- Stimare la **frequenza** degli incidenti informatici
- Stimarne la **gravità** (il costo economico o almeno la quantità di dati compromessi)
- Stimare le perdite dovute ad **eventi estremi** (VaR, TVaR)

Evidenze dalla letteratura

- La maggioranza degli studi considera **database pubblici**
  - Probabile sottostima del fenomeno
  - Mancanza di informazione sul danno economico
- La distribuzione delle perdite ha **code alte** e questo fenomeno è **robusto**
- La severità degli incidenti è differente per differenti tipi di organizzazione
- Gli episodi meno severi sono in genere sottorappresentati
- Il costo economico di un incidente …

Un esempio

Una organizzazione non-profit fondata nel 1992



L'archivio degli incidenti riporta ~10k eventi in US, raccolti da US Attorneys general, Department of Health and Human Services e confermati dai principali media

- dal 1 gennaio 2005 al 31 dicembre 2019
- nome, sede e tipo di organizzazione
- descrizione e tipo dell'incidente
- (spesso) numero di dati compromessi

Cosa si intende per violazione dei dati personali (data breach)?

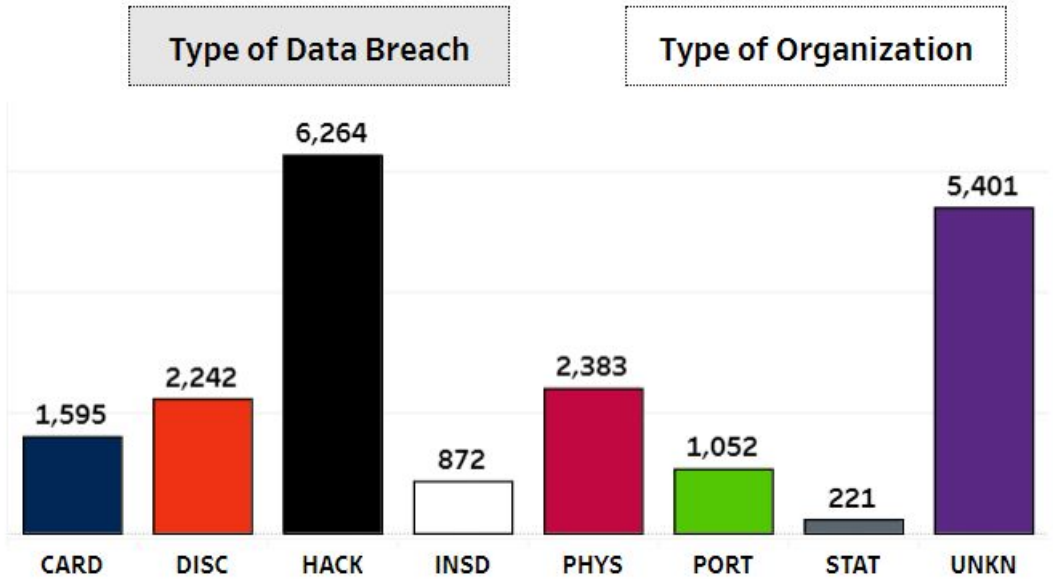
Una violazione di sicurezza che comporta - accidentalmente o in modo illecito - la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

Una violazione dei dati personali può compromettere la riservatezza, l'integrità o la disponibilità di dati personali.

La violazione dei dati è la causa maggiore di incidenti informatici (Allianz Risk Barometer).

Il costo medio di un singolo data breach nel 2022 è stato di circa $4.35mn ed entro la fine del 2023 supererà i $5mn.

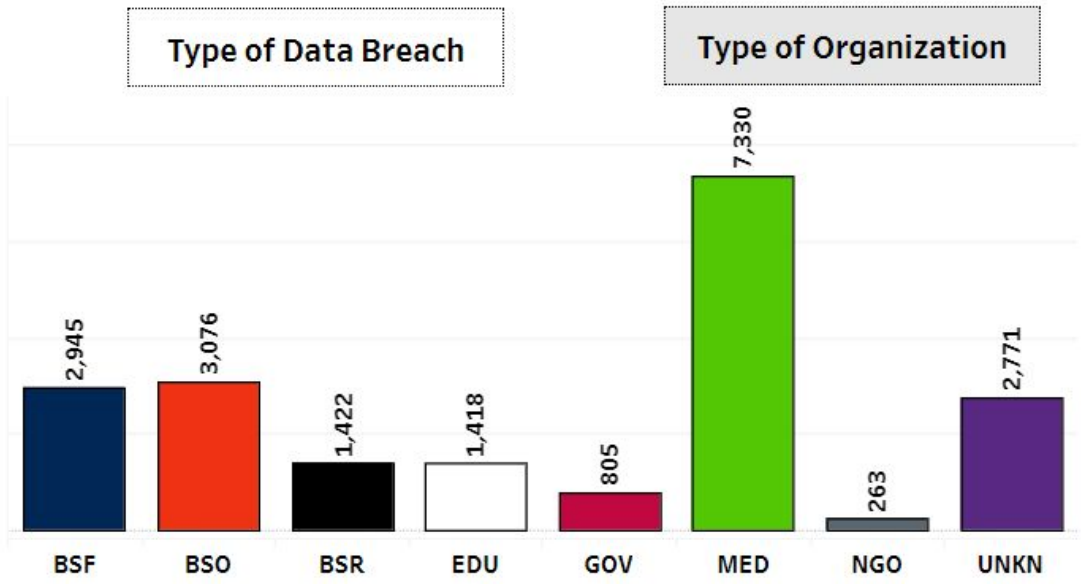
Tipo di incidente



- CARD - Debit and Credit Cards Not Via Hacking
- HACK - Hacked by an Outside Party or Infected by Malware
- INSD - Insider (employee, contractor or customer)
- PHYS - Physical (paper documents that are lost, discarded or stolen)
- PORT - Portable Device (lost, discarded or stolen laptop, smartphone, memory stick, CDs, hard drive, data tape, etc.)
- STAT - Stationary Computer Loss (lost, inappropriately accessed, discarded or stolen computer or server not designed for mobility)
- DISC - Unintended Disclosure Not Involving Hacking, Intentional Breach or Physical Loss (sensitive information posted publicly, mishandled or sent to the wrong party via publishing online, sending in an email or sending via fax)
- UNKN - Unknown (not enough information about breach to know how exactly the information was exposed)

Tipo di organizzazione

- BSF - Businesses (Financial Services, Banking, Insurance Services)
- BSO - Businesses (Manufacturing, Technology, Communications, Other)
- BSR - Businesses (Retail/Merchant including Grocery Stores, Online Retailers, Restaurants)
- EDU - Educational Institutions (Schools, Colleges, Universities)
- GOV - Government & Military (State & Local Governments, Federal Agencies)
- MED - Healthcare and Medical Providers (Hospitals, Medical Insurance Services)
- NGO - Nonprofits (Charities and Religious Organizations)
- UNKN – Unknown



Dati dal 2010 al 2019

Numero di incidenti

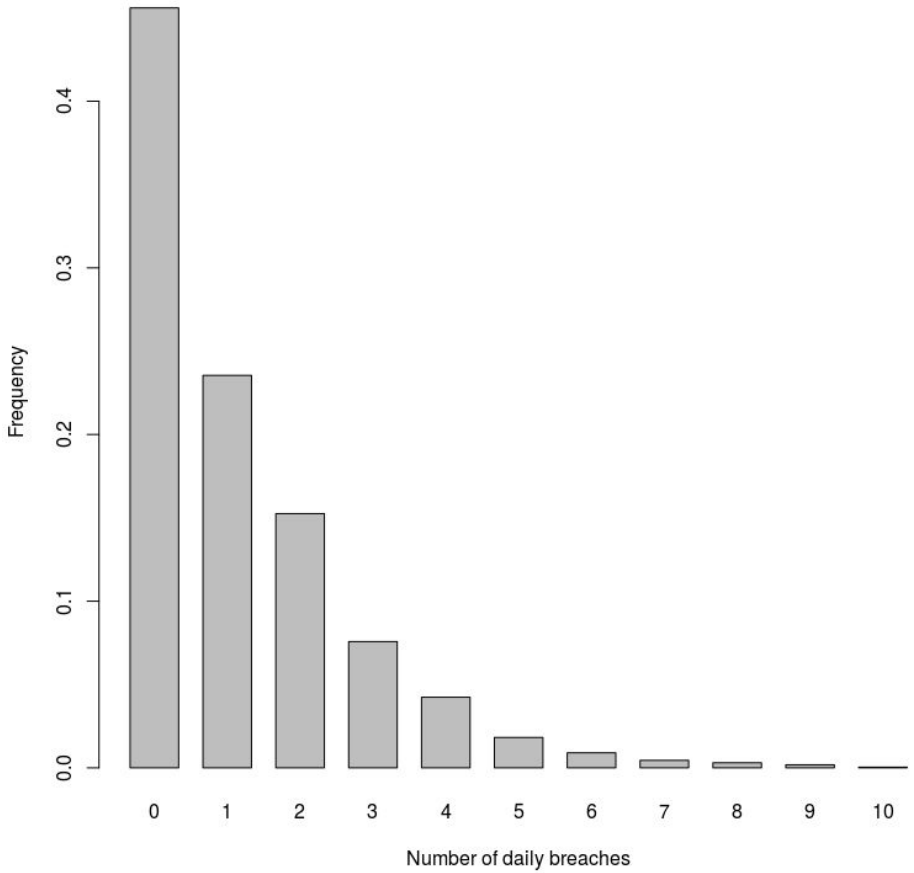
	BSF	BSO	BSR	EDU	GOV	MED	NGO	UNKN	TOTAL
#N/A	0	0	0	0	0	87	0	0	87
CARD	8	2	15	1	0	0	0	0	26
DISC	39	33	34	83	85	991	5	0	1270
HACK	78	188	113	102	68	798	20	0	1367
INSD	29	15	32	8	36	160	5	0	285
PHYS	11	14	5	15	31	1281	5	0	1362
PORT	16	23	10	31	46	289	10	0	425
STAT	3	3	2	6	2	72	0	0	88
UNKN	41	11	7	34	14	32	2	465	606
TOTAL	225	289	218	280	282	3710	47	465	5516

Numero di dati (10G)

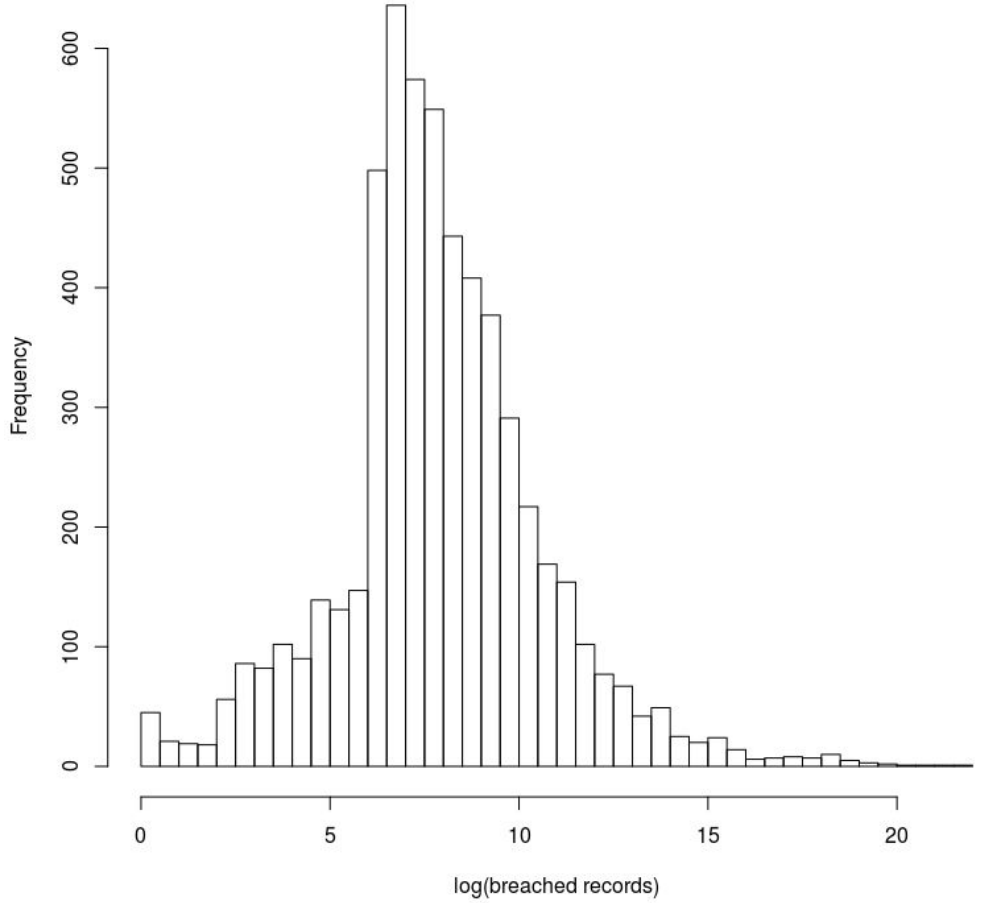
	BSF	BSO	BSR	EDU	GOV	MED	NGO	UNKN
#N/A	0	0	0	0	0	3079889	0	0
CARD	7035066	310	2124575	16	0	0	0	0
DISC	1550375	2105006706	385194087	1576141	21094488	12979387	3501561	0
HACK	348057288	5494774684	791295680	45231810	40900705	159979906	3350944	0
INSD	2407569	3508456	35671	40379	28506293	1059014	317	0
PHYS	58909	64007	4071	1023422	209616	35715718	24157	0
PORT	5852045	5836258	30244	238778	7683283	12645645	72176	0
STAT	100348	80108	9189	78177	3650	9604567	0	0
UNKN	421366	100155387	68000391	10352675	849587	109731	2501	10657026

Caratterizzare incidenti - frequenza e gravità

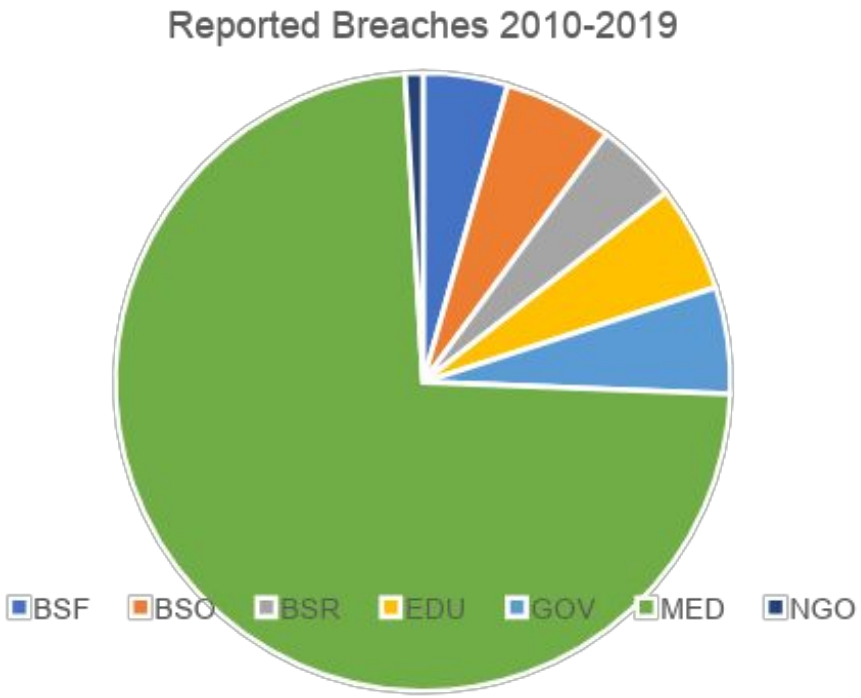
Frequenza degli incidenti

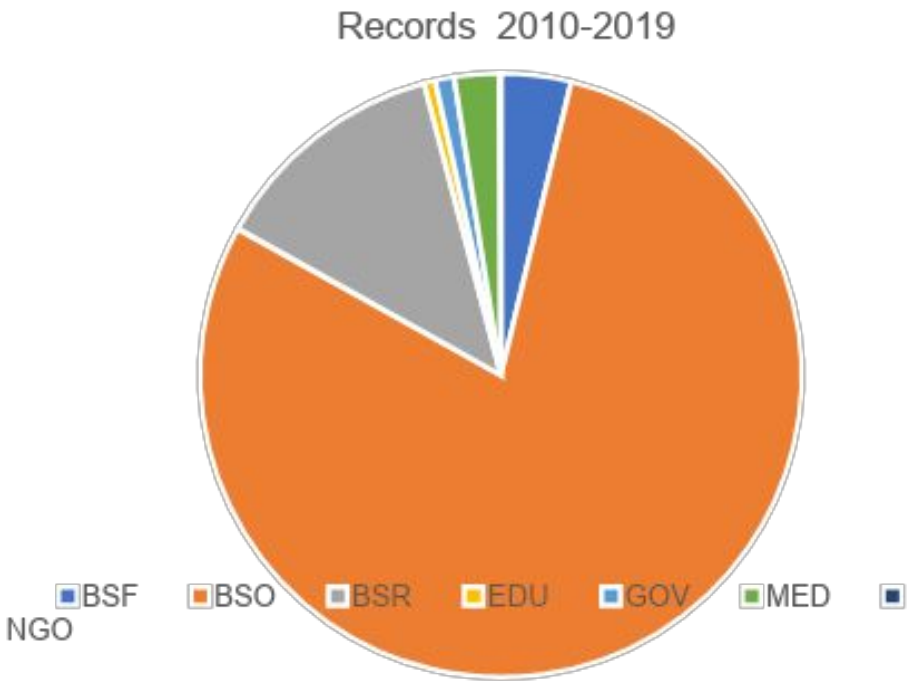


Gravità degli incidenti

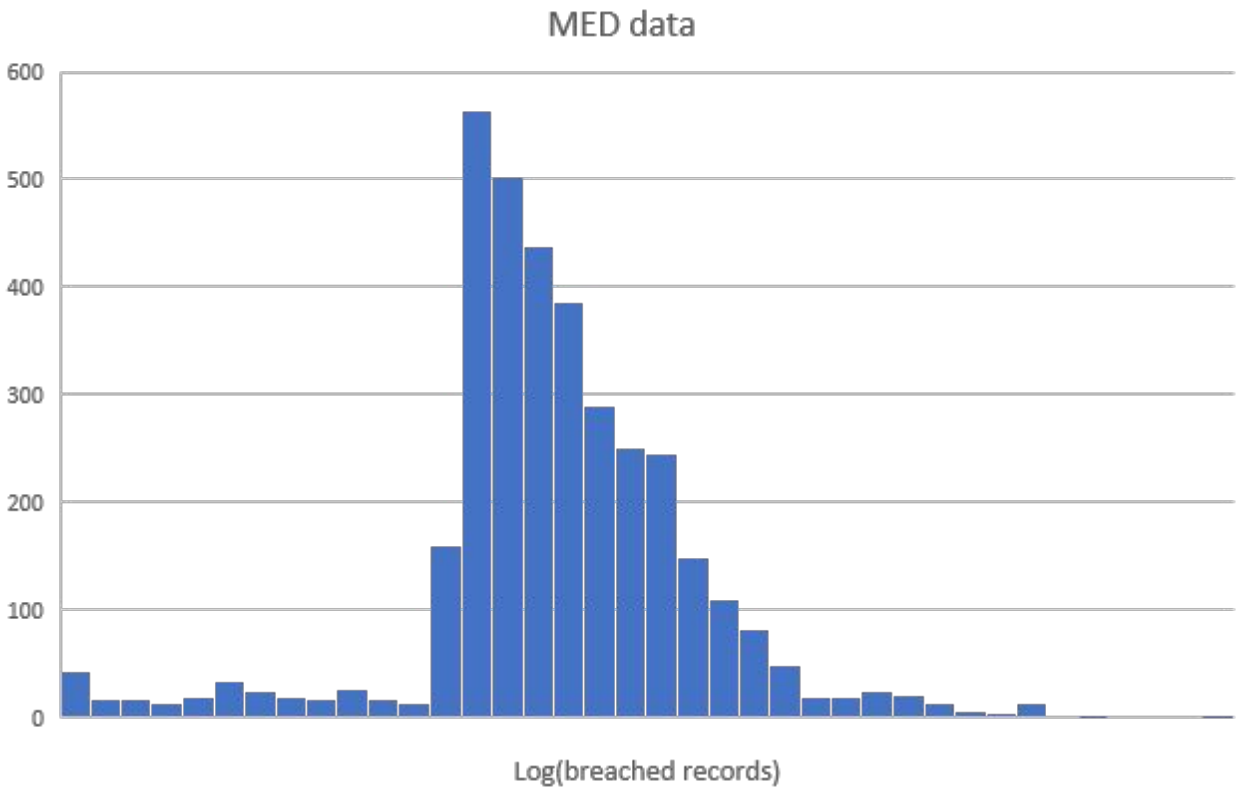


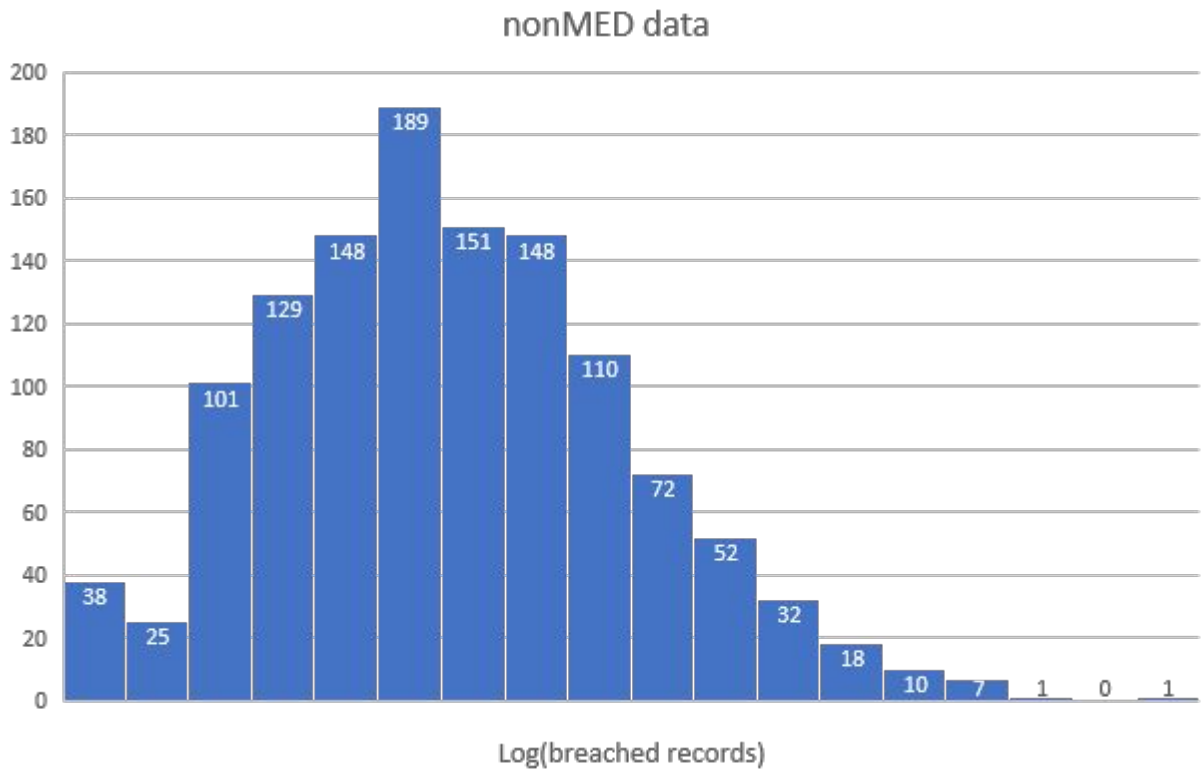
Numero di incidenti e volume di dati compromessi dal 2010 al 2019 per tipo di organizzazione





Severità degli incidenti (2010-2019)

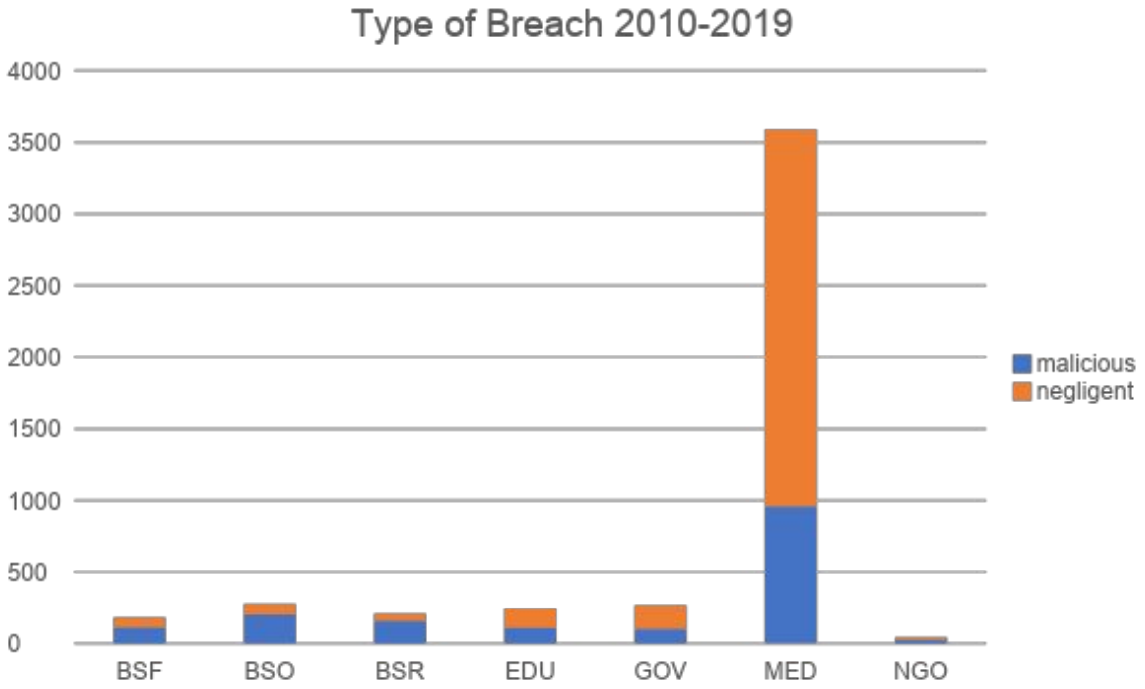


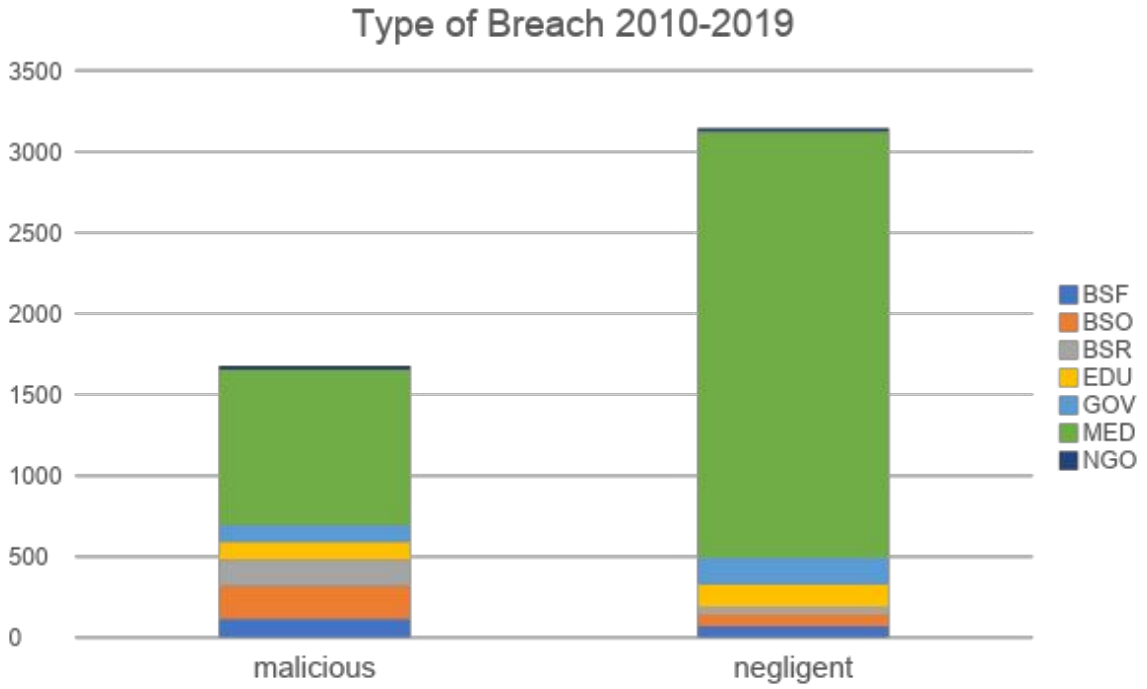


Distinguiamo due tipologie di incidente:

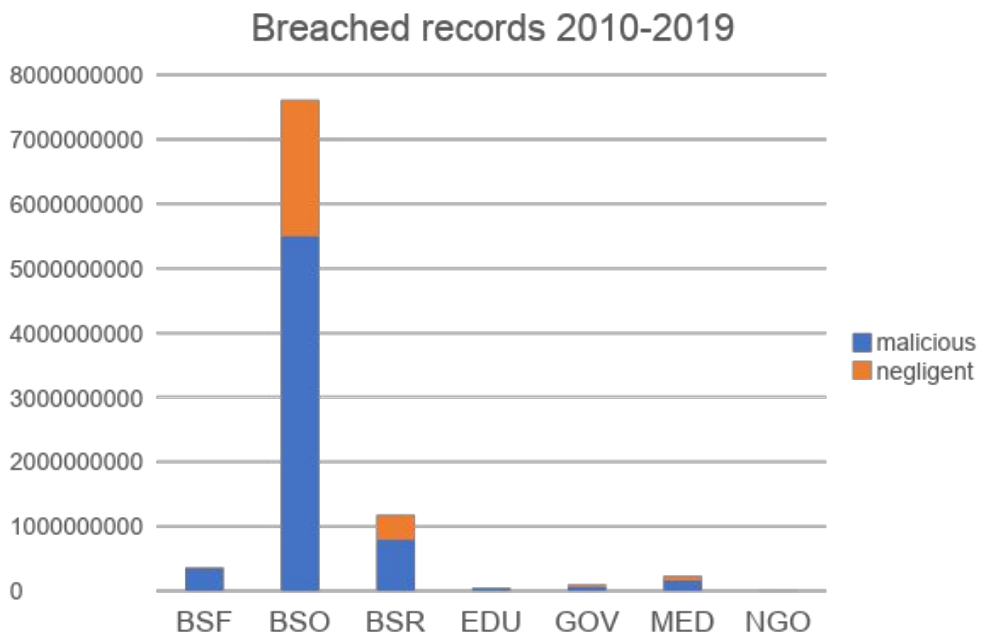
- Causati da disattenzione, esposizione involontaria o mancata vigilanza (**negligent**)
  - **PHYS** - Physical (documents that are lost, discarded or stolen)
  - **PORT** - Portable Device (lost, discarded or stolen laptop, smartphone, memory stick, CDs, hard drive, data tape, etc.)
  - **STAT** - Stationary Computer Loss (lost, inappropriately accessed, discarded or stolen computer or server not designed for mobility)
  - **DISC** - Unintended Disclosure (sensitive information posted publicly, mishandled or sent to the wrong party via publishing online, sending in an email or sending via fax)
- Causati da un attacco intenzionale alle informazioni sensibili (**malicious**)
  - **CARD** - Debit and Credit Cards Not Via Hacking
  - **HACK** - Hacked by an Outside Party or Infected by Malware
  - **INSD** - Insider (employee, contractor or customer)

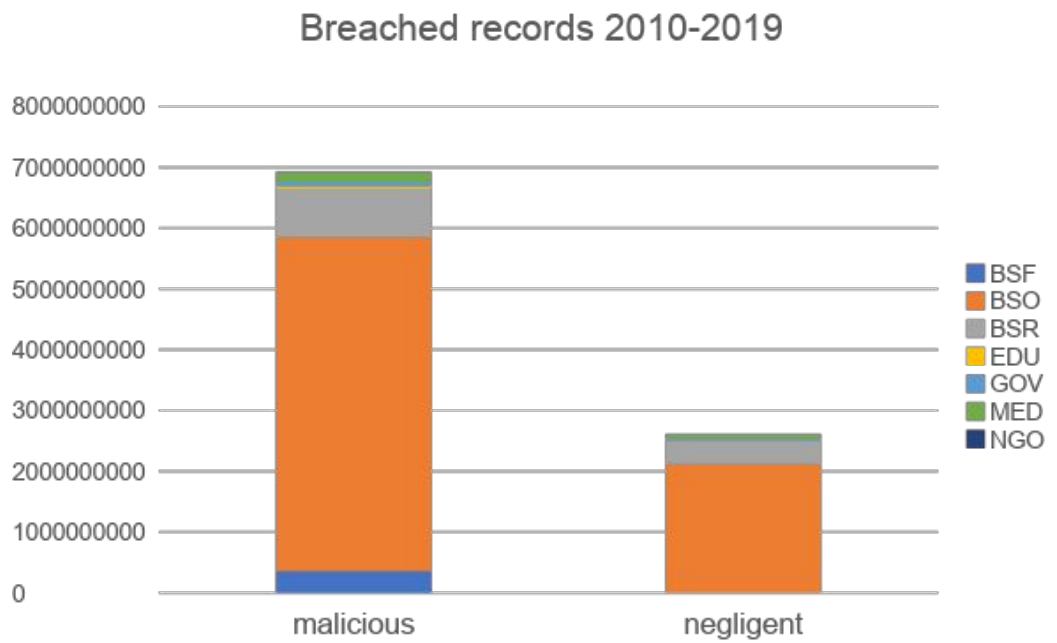
Numero di incidenti (2010-2019)



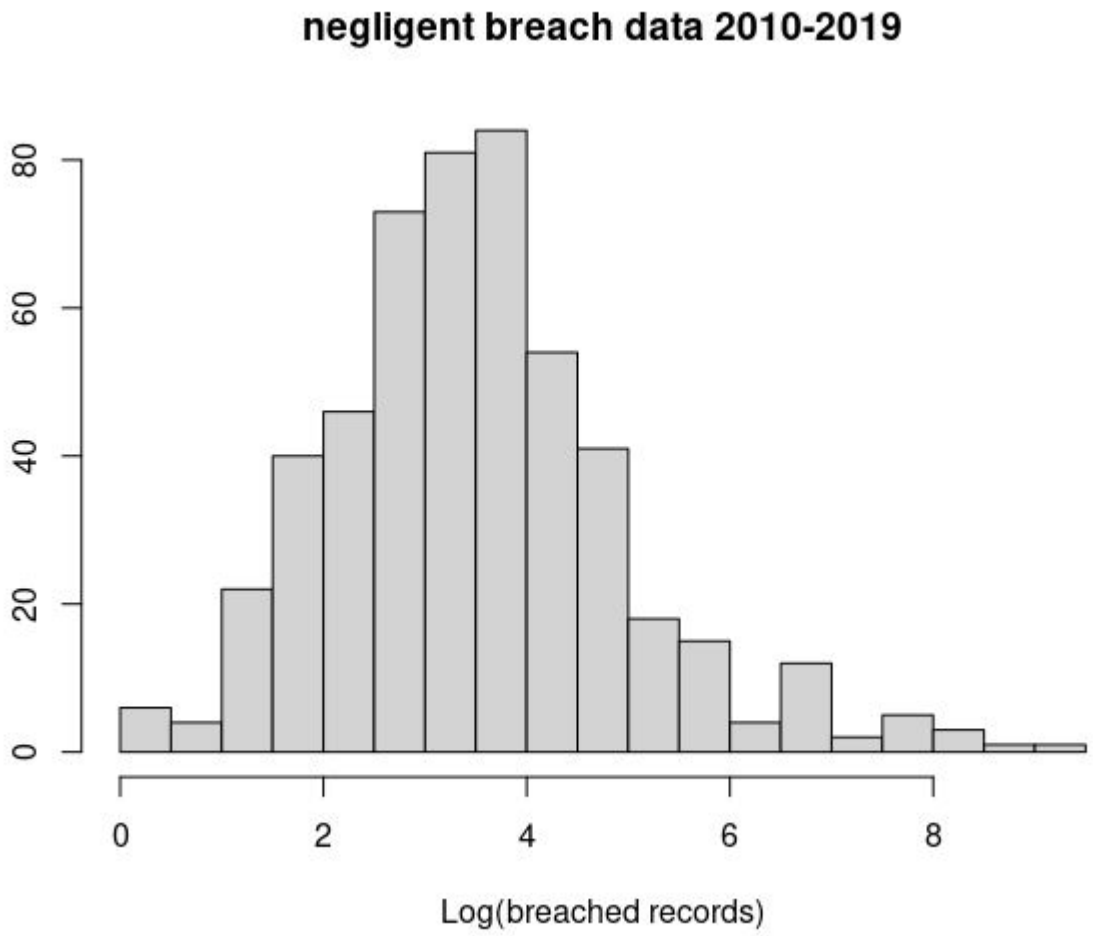


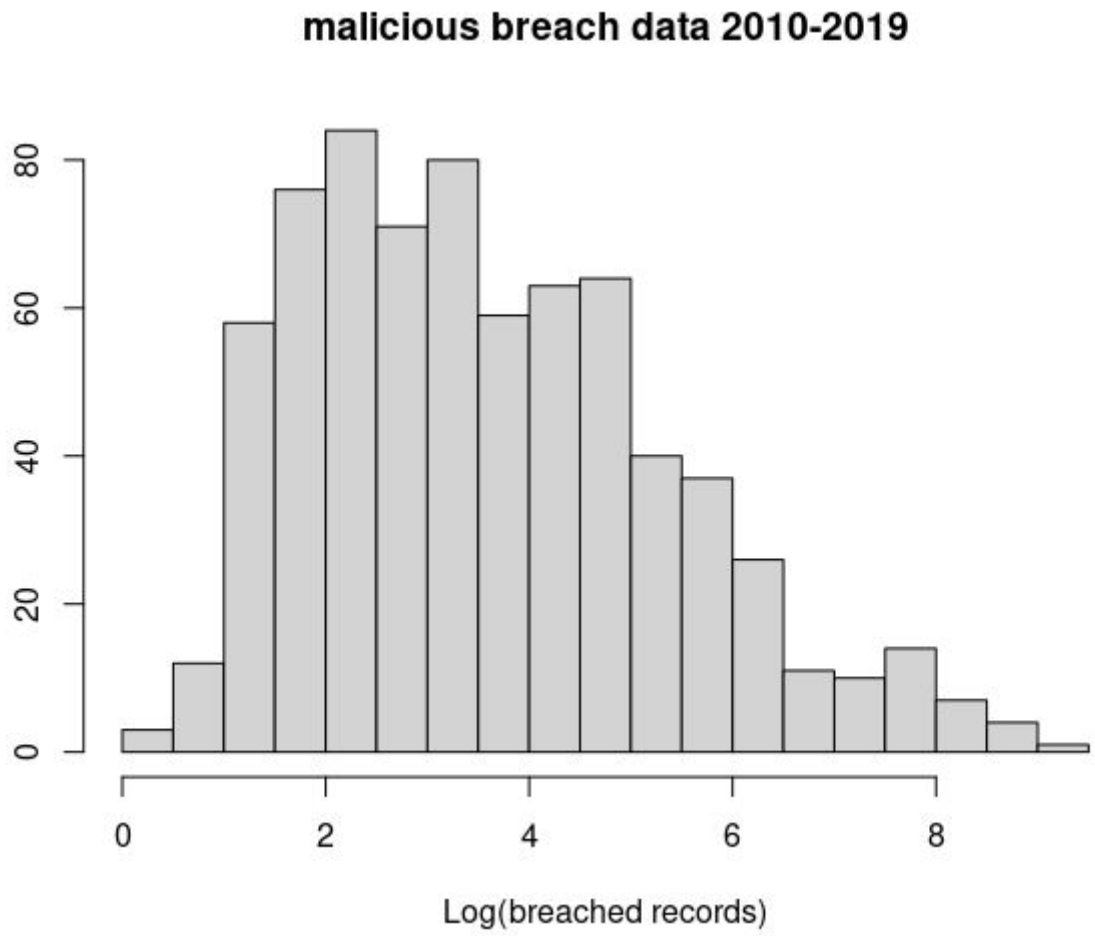
Severità degli incidenti (2010-2019)





Severità dei breaches nelle organizzazioni nonMED

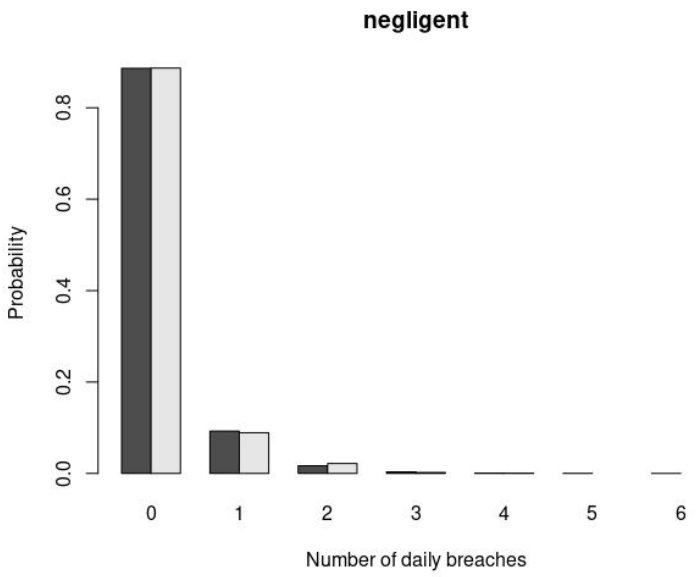


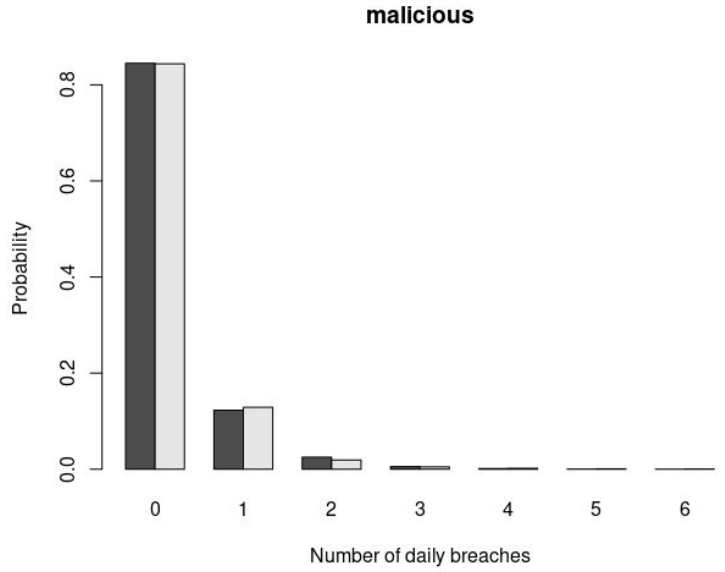


Caratterizzare incidenti - frequenza

Il modello statistico per la frequenza temporale degli incidenti è una distribuzione discreta che rappresenti la probabilità di osservare 0,1,2,… eventi nell'unità di tempo fissata (giorno, settimana,…)
solitamente in letteratura si utilizza una Poisson o una binomiale negativa.

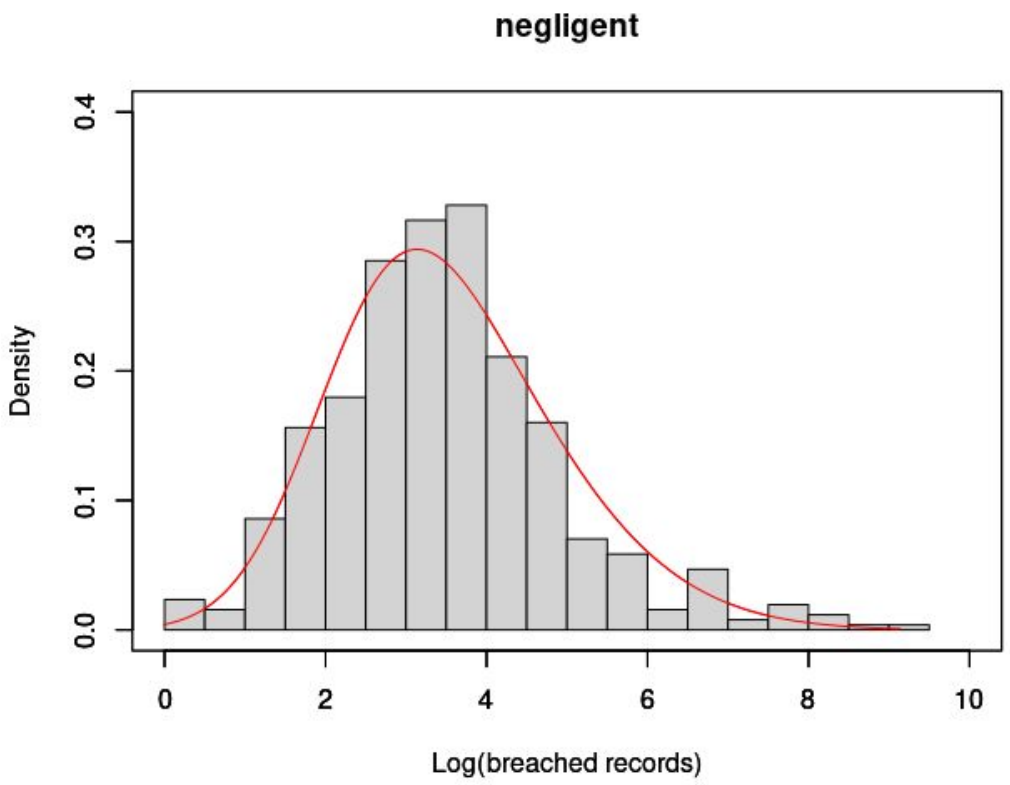
- Abbiamo provato entrambe e testato la bontà di adattamento, che è risultata migliore per la **binomiale negativa**, che meglio rappresenta eventi così eterogenei.
- Abbiamo verificato la bontà di adattamento con un test statistico (KS) che ha confermato l'ottimo accordo.

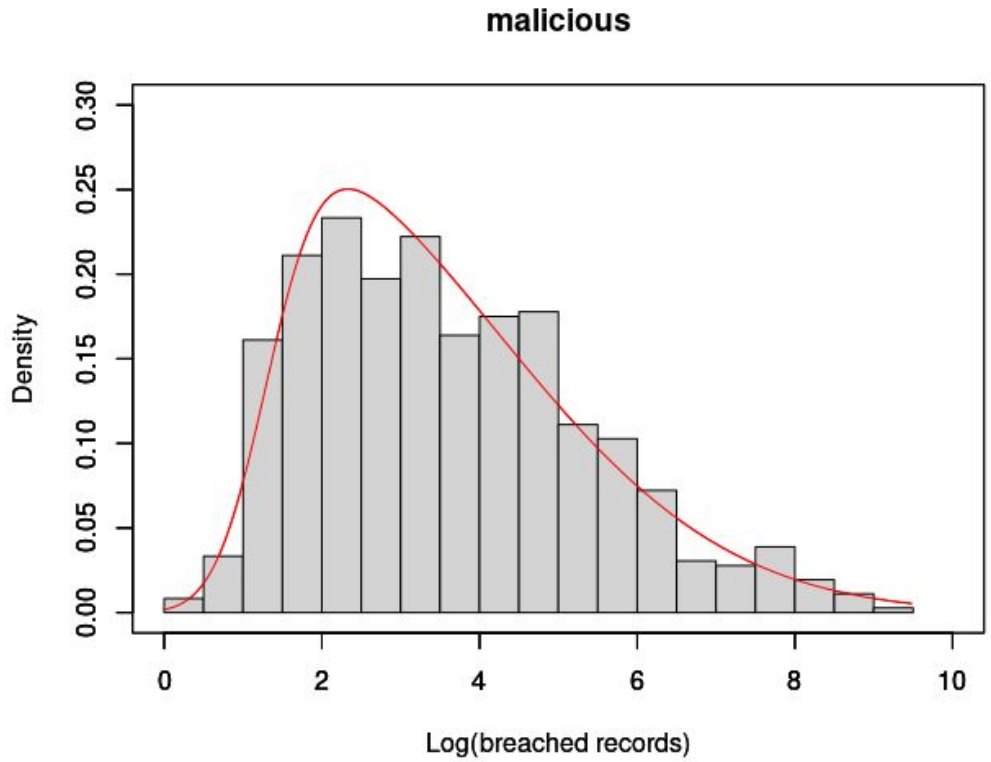




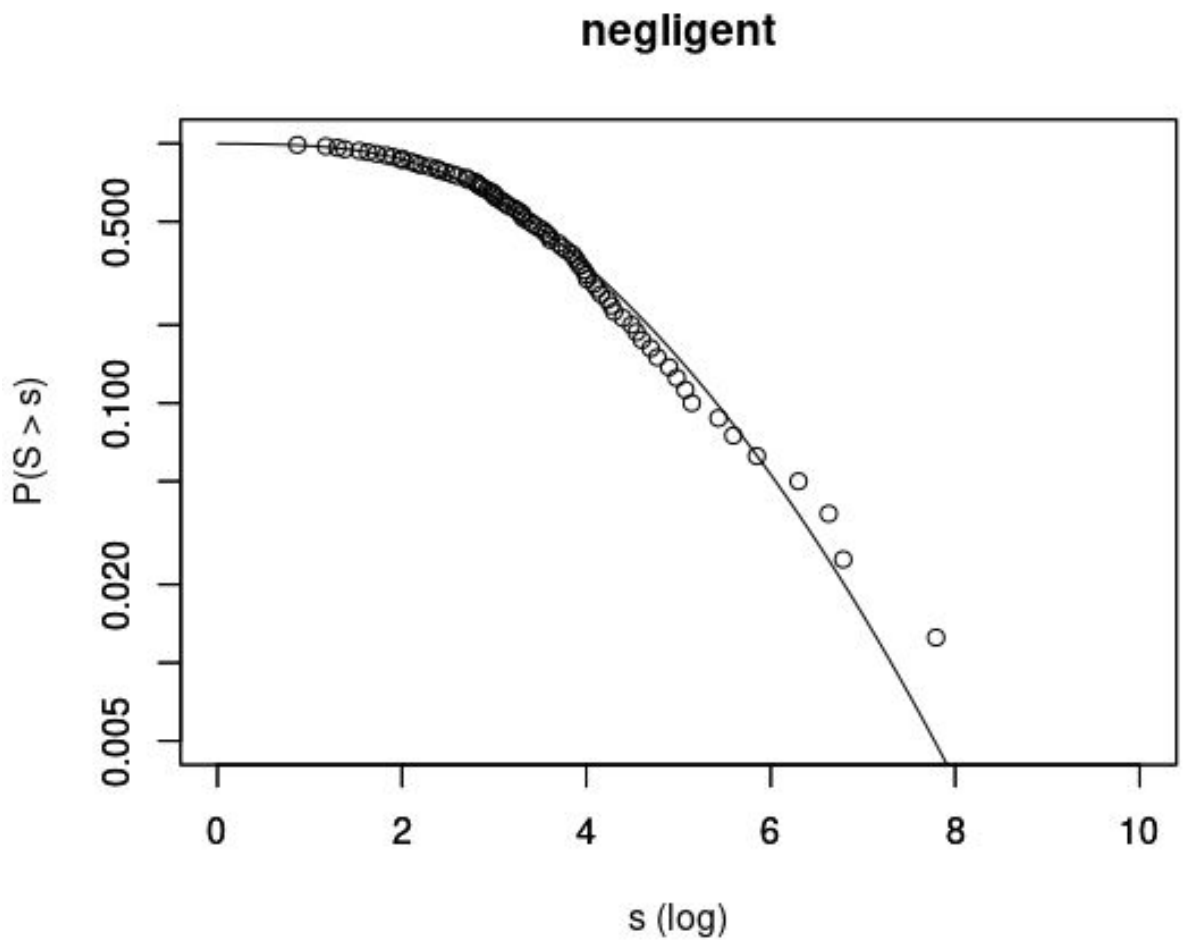
Caratterizzare incidenti - gravità

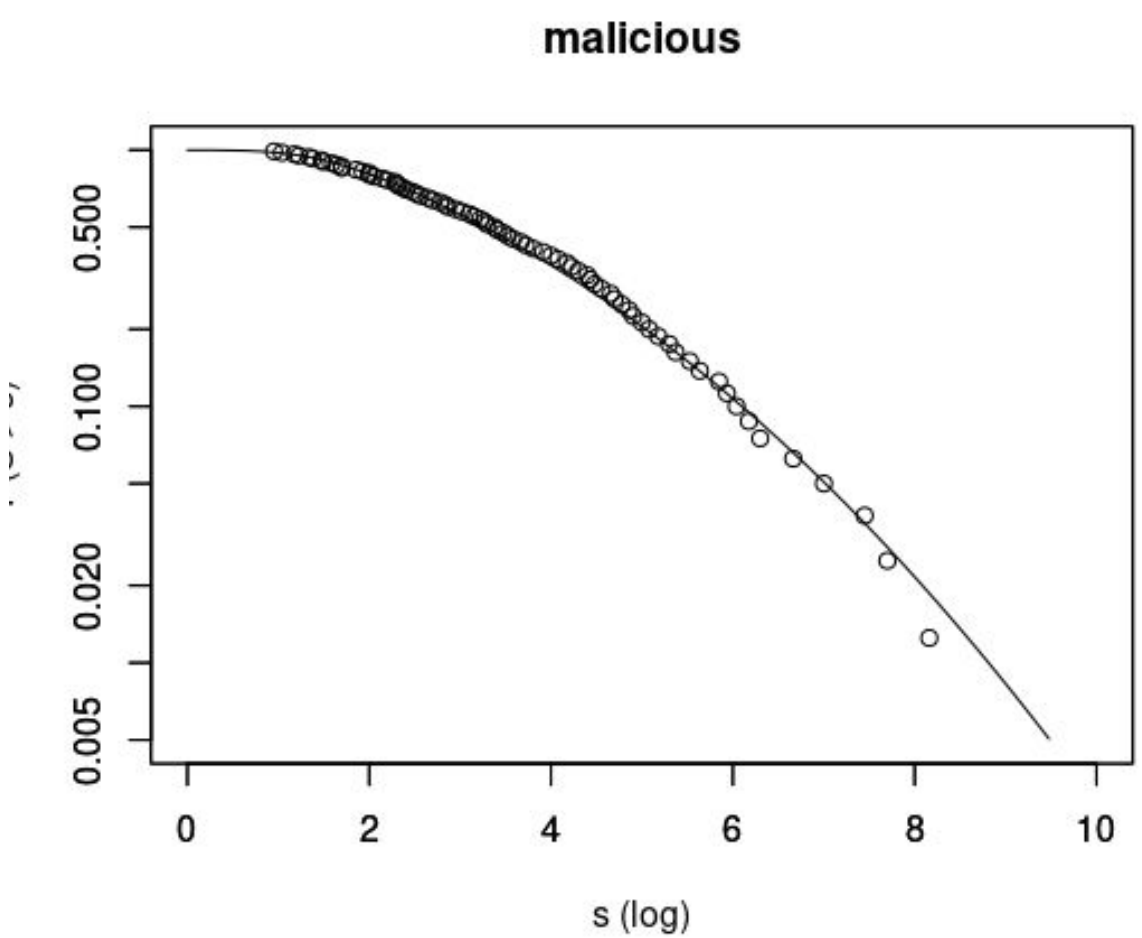
Il modello statistico per la gravità degli incidenti è una distribuzione che rappresenti l'intensità osservata degli eventi, espressa dal numero di dati compromessi.
Si tratta di valori positivi, per cui i modelli più usati sono la distribuzione lognormale e la skew-normal.
Abbiamo provato entrambe e testato la bontà di adattamento, che è risultata migliore per la skew-normal.





Analizziamo le code delle due distribuzioni





Stima del VaR e del TVaR

Occorre modellare le perdite aggregate, cioè il totale delle perdite in un determinato periodo.

Accenniamo a due approcci diversi, comuni nella letteratura attuariale e da noi esplorati:

- L'**approccio storico** assume la stazionarietà della distribuzione delle perdite aggregate e quindi la ricostruisce come la distribuzione empirica dei dati finora osservati
- L'**approccio simulativo** (Monte Carlo) utilizza le distribuzioni stimate della frequenza e della severità degli incidenti e campiona nel periodo considerato numero e severità degli incidenti per costruire la distribuzione delle perdite aggregate.

Prospettive future

DATI

- Arricchire il dataset attraverso la fusione con altri dataset pubblici
- Utilizzare dati europei, a partire dal dataset delle sanzioni per violazioni del GDPR

METODOLOGIA STATISTICA

- Extreme Value Theory
- Esplorare modelli di relazione tra frequenza e severità

RICADUTE ECONOMICO-FINANZIARIE

- Considerare il punto di vista dell'azienda vittima di incidente informatico per valutare la convenienza economica dell'investimento in sicurezza e dell'investimento in assicurazione

Riferimenti bibliografici

- Carfora, M.F.; Orlando, A. Some Remarks on Malicious and Negligent Data Breach Distribution Estimates. *Computation* 2022, 10, 208
- Carfora, M.F.; Orlando, A. Quantile based risk measures in cyber security. In *Proceedings of the 2019 International Conference on Cyber Situational Awareness, Data Analytics and Assessment* (Cyber SA), Oxford, UK, 3–4 June 2019; pp. 1–4.
- Carfora, M.F.; Martinelli, F.; Mercaldo, F.; Orlando, A. Cyber Risk Management: An Actuarial Point of View. *J. Oper. Risk* 2019, *14*, 77–103.
- Marotta, A.; Martinelli, F.; Nanni, S.; Orlando, A.; Yautsiukhin, A. Cyber-insurance survey. *Comput. Sci. Rev.* 2017, *24*, 35–61
- Eling, M.; Loperfido, N. Data breaches. Goodness of fit, pricing, and risk measurement. *Insur. Math. Econ.* 2017, *75*, 126–136.
- Edwards, B.; Hofmeyr, S.; Forrest, S. Hype and heavy tails: A closer look at data breaches. *J. Cybersecur.* 2016, *2*, 3–14.