Privacy by design significa anche per voi “sicurezza senza fare niente»?

Luca Bechelli

Information & Cyber Security Advisor

Direttivo e Comitato Tecnico - Scientifico CLUSIT

I numeri della bestia

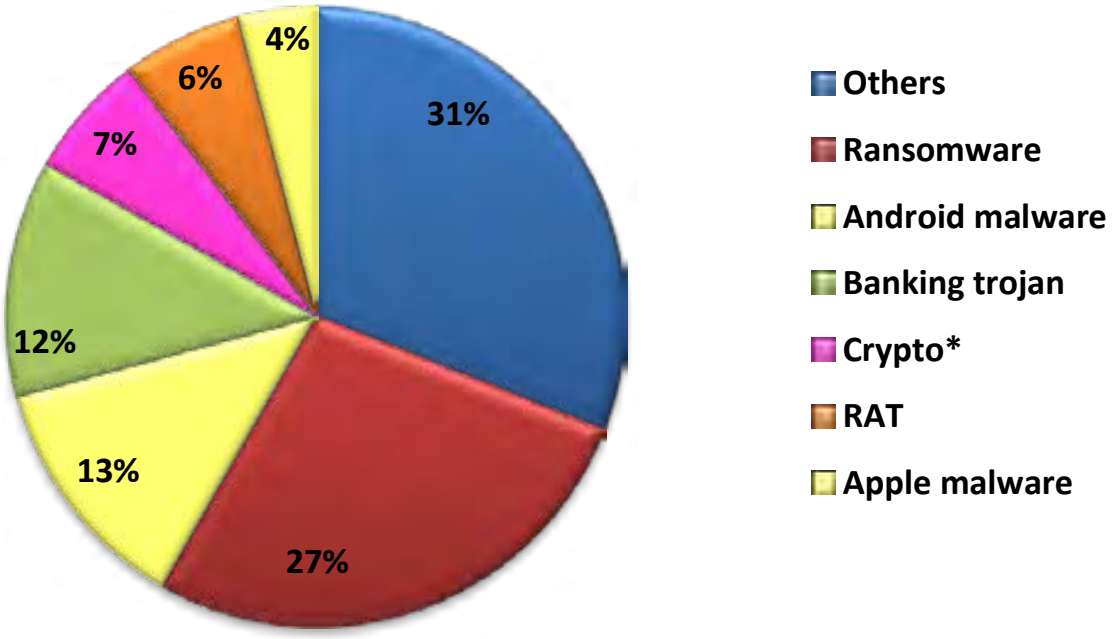
94 attacchi gravi al mese

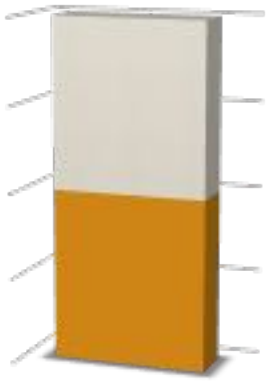
+7% degli attacchi, rispetto all'anno precedente

+14% attacchi di cybercrime

Colpa «loro»?!?

+94% attacchi malware «comune»



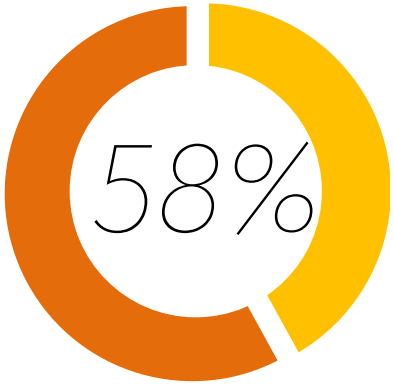


50%

of the worst breaches of the year were caused by inadvertent human error.

PWC Information Security Breaches Survey 2015

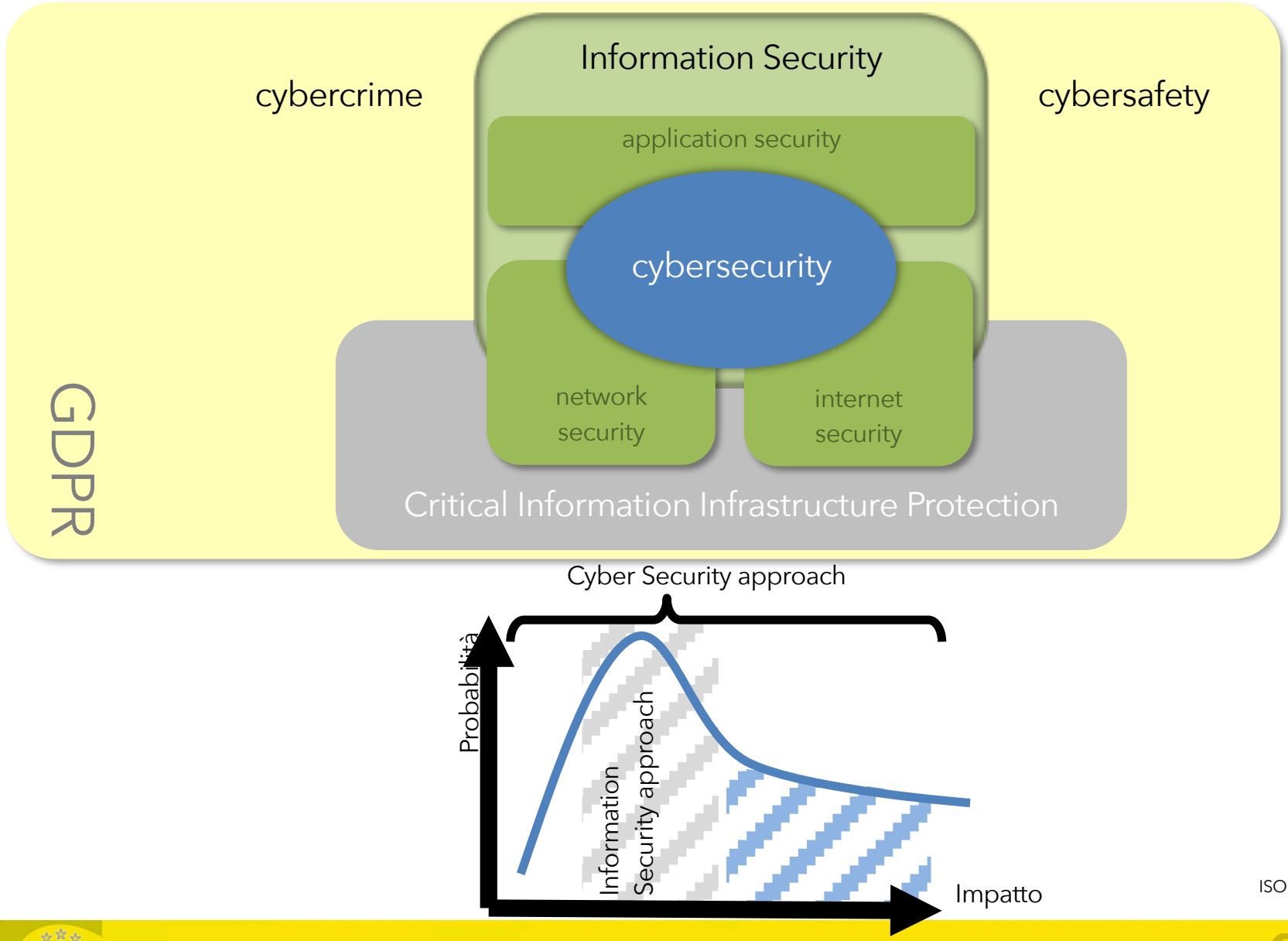

Segnali Deboli:
+6% APT



Delle imprese in EU a fronte della domanda di cosa è stato implementato in termini di politiche-procedure di sicurezza IT, risponde con "controllo delle vulnerabilità"

Quando manca il risk management

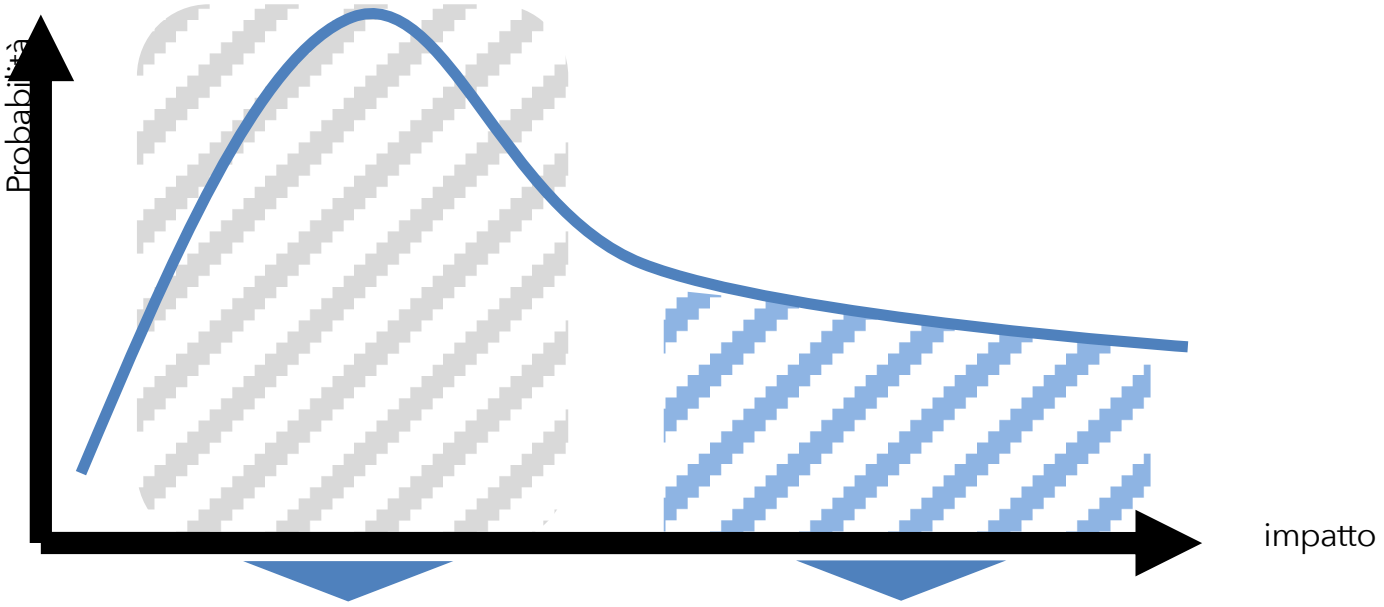
Come (dovrebbe) evolve(re) l'approccio della security aziendale



ISO 27032:2012

http://www.isaca.org/Knowledge-Center/Blog/Lists/Posts/Post.aspx?ID=296

Approcci tradizionali: principali limiti…



- Complesso in termini di progettazione e attuazione
- Esposto a errori di valutazione soggettiva
- Indirizza prevalentemente interventi "verticali"
- Rappresentabile al management, soprattutto in chiave quantitativa
- Bassa frequenza di attuazione

Valore limitato nel tempo

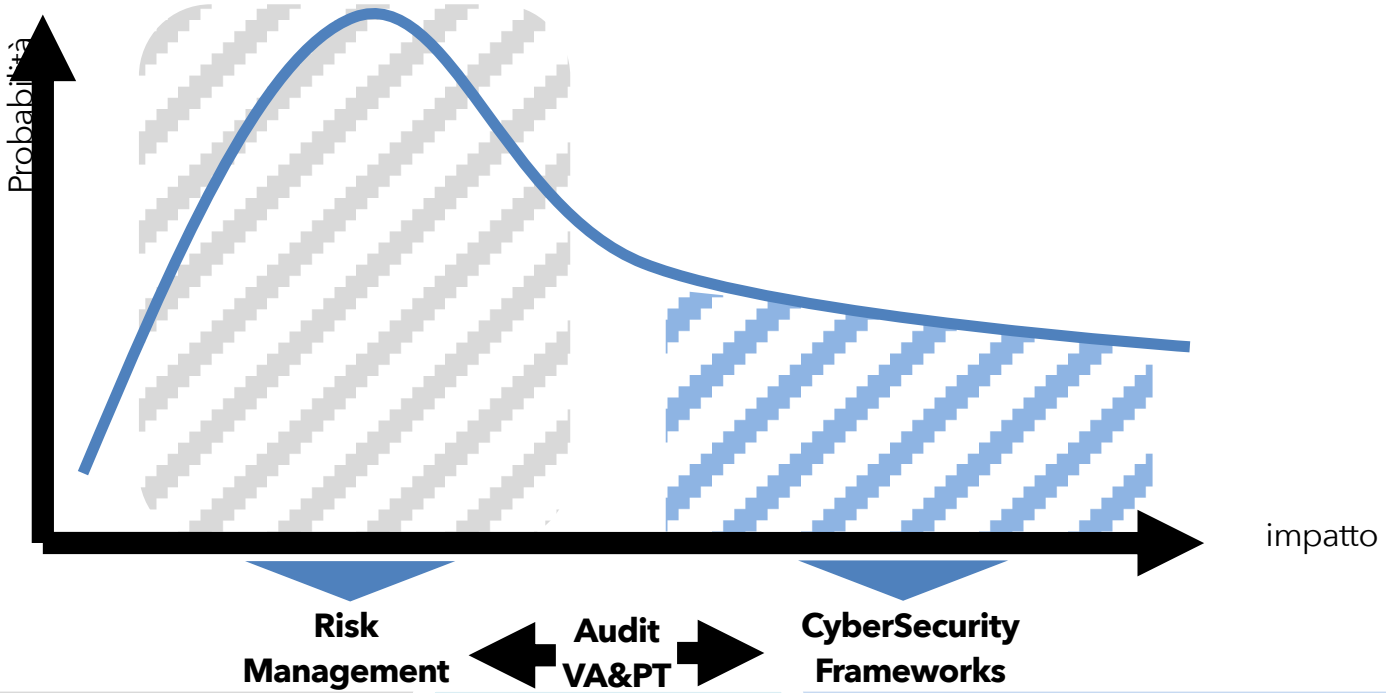
Audit: richiedono un modello di riferimento

Indirizzano remediation "tecniche/operative"

Alta frequenza di attuazione, limitata solo dai tempi di remediation

- Approccio "checklist": misuro quanto mi difendo, non quanto è efficace la difesa
  - Modelli di riferimento scarsamente personalizzati
  - Modelli non proporzionali
    - Controlli di natura tecnica
    - Alta frequenza di attuazione (limitata solo dai tempi di remediation)

…concretamente (di solito)…



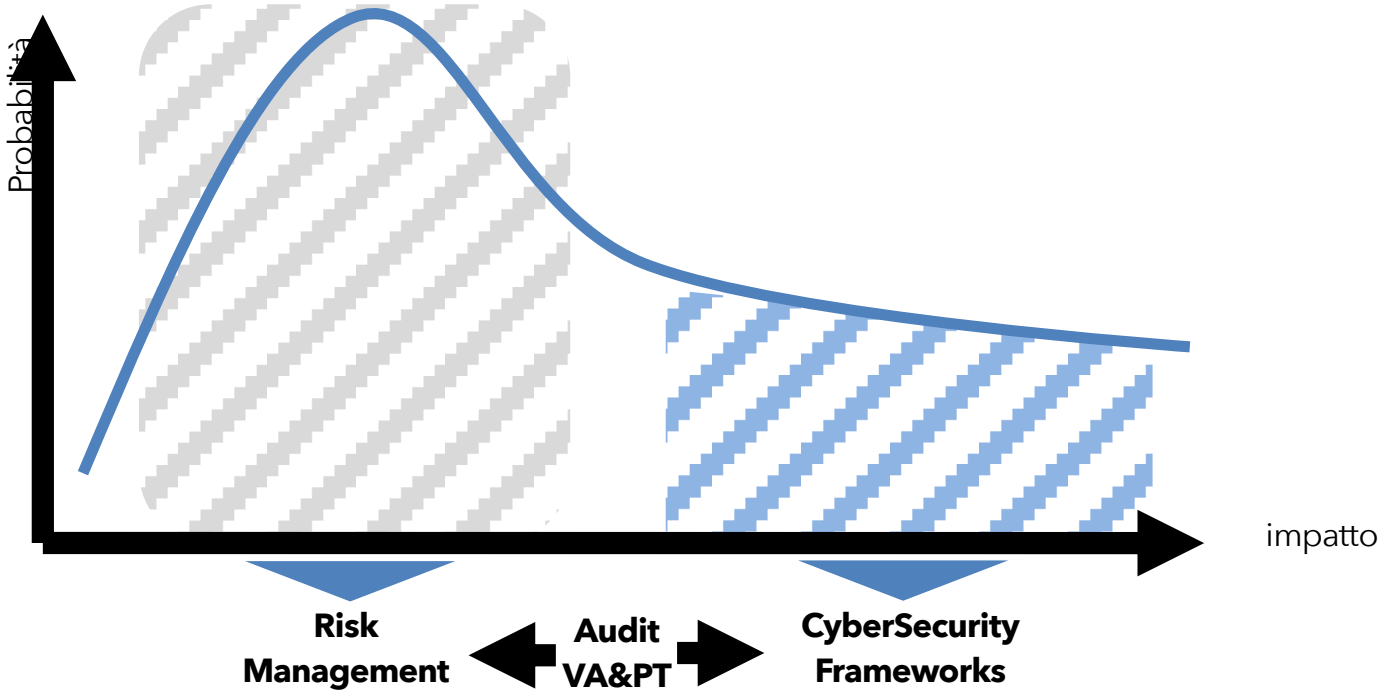
- Scarso coinvolgimento del business e altrettanto scarsa condivisione e comprensione dei risultati
- Elevata attenzione agli aspetti metodologici, limitata linearità tra input e risultati dell'analisi
- Limitata attenzione ai "fattori di rischio" a favore di un'eccessiva ricerca di criteri oggettivi per valutare rischi noti
- Scarsa reattività

Risolvono problemi noti a partire da obiettivi altrettanto noti

Costituiscono uno strumento di sensibilizzazione del management

- In assenza di altri strumenti o modelli di governo della sicurezza e dei rischi, supportano l'azienda nell'individuazione di interventi ad alta priorità a fronte dell'escalation delle minacce esterne verificatasi negli ultimi anni
- Elevata reattività
- Per il business: "l'ha detto il NIST"

Cosa manca?



- Partecipazione del management nella fase di analisi / assessment
- Recepimento e condivisione delle effettive esigenze / obiettivi
- Rappresentazione dei risultati in forma comprensibile (soprattutto dei razionali che individuano le maggiori criticità, **#checcifregaselodiceilNIST**, **#laCIAciSpia**, **#piùPentoleXtutti**….)
- Correlazione delle criticità con gli impatti
- Ambito di ricerca delle azioni di mitigazione che comprenda sia il business che l'IT, sia il sistema Informat**ICO** che **InformatIVO**

Privacy by design

Descritta da sette principi, definiti negli anni '90 (in particolare nel 1995):

- Proactive not Reactive: The PbD approach attempts to anticipate and prevent privacy-invasive events before they happen.
- Privacy as the Default Setting: Ensure that personal data is automatically protected in any given IT system or business practice, ***so that if an individual does nothing, their privacy still remains intact***.
- Privacy Embedded into Design: Privacy should be embedded into the design and architecture of IT systems and business practices.
- Full Functionality – Positive-Sum, not Zero-Sum: PbD seeks to accommodate all legitimate interests and objectives in a "win-win" manner, balancing seemly opposing interests, such as security and privacy.
- End-to-End Security – Full Lifecycle Protection: PbD extends throughout the entire lifecycle of the data involved, from start to finish.
- Visibility and Transparency: It seeks to assure all stakeholders that component parts and operations remain visible and transparent, to users and providers alike.
- Respect for User Privacy – Keep it User-Centric: Above all, it puts the interests of the individual by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options.

https://www.ipc.on.ca/privacy/protecting-personal-information/privacy-by-design/

. . .e la privacy?!?

Privacy by Design

- Art.25 – Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita:
  - tenendo conto dello stato dell'arte e dei costi di attuazione, nonche´della natura, dell'ambito di applicazione, del contesto e delle finalita`del trattamento, come anche dei **rischi aventi probabilita`e gravità** diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, **sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso** il titolare del trattamento **mette in atto misure tecniche e organizzative adeguate**, quali la pseudonimizzazione, **volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione**, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati.

Obiettivi da perseguire…

- **correttezza e trasparenza**: i dati saranno trattati in modo corretto e trasparente nei confronti dell'interessato, in particolare prevedendo informative adeguate prima di intraprendere qualsiasi trattamento e successive comunicazioni riguardo ad eventuali modifiche rispetto a quanto inizialmente indicato;

- **limitazione della finalità**: i dati saranno raccolti esclusivamente per finalità determinate, esplicite e legittime e successivamente trattati in modi che non siano incompatibili con tali finalità;

- **liceità**: i dati saranno raccolti e trattati, ad eccezione dei casi tassativi esplicitamente previsti dal Regolamento, solo in presenza di una o più delle condizioni di liceità da quest'ultimo identificate;

- **esattezza**: i dati devono essere mantenuti esatti e, se necessario, aggiornati. Pertanto, dovranno sussistere tutte le misure necessarie a cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati;

- **minimizzazione dei dati**: i dati devono essere adeguati, pertinenti e limitati a quanto strettamente necessario alla realizzazione delle finalità per cui saranno raccolti;

- **limitazione della conservazione**: i dati saranno conservati in una forma che consentirà l'identificazione degli interessati per un arco di tempo non superiore a quello necessario al conseguimento delle finalità per le quali sono stati raccolti e trattati;

- **responsabilizzazione**: l'azienda dovrà essere in grado di comprovare l'adozione di misure e processi idonei a garantire il rispetto dei principi descritti ai punti che precedono, delle norme del GDPR (accountability) e delle misure individuate sulla base dell'analisi dei rischi.

Ciclo di vita del trattamento e analisi del rischio

Trattamenti ad alto Rischio

Art.35 (DPIA):

- Un insieme di azioni, tra cui l'Analisi del rischio:
  - Valutazione impatti e probabilità
  - Identificazione misure
- eventuale "consultazione preventiva"

Art.35 (DPIA), comma 11:

- *"**Se necessario**, il titolare del trattamento procede a un **riesame** per valutare se il trattamento dei dati personali sia effettuato conformemente alla valutazione d'impatto sulla protezione dei dati almeno quando insorgono variazioni del rischio rappresentato dalle attività relative al trattamento"*
- Il WP29 suggerisce una frequenza al più triennale

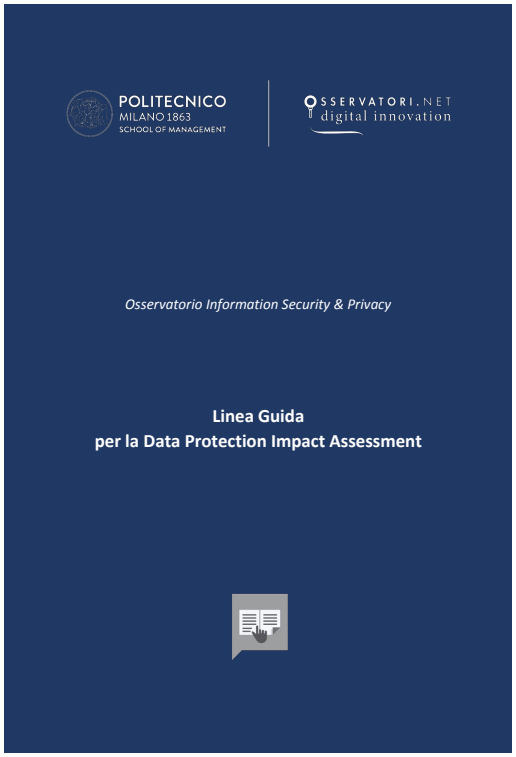
In tutti i casi

Art.25 (privacy by design / default):

- Analisi del rischio:
  - Valutazione impatti e probabilità
  - Identificazione misure
- Implementazione

Art.32 (sicurezza del trattamento):

- Aggiornamento **periodico** dell'Analisi del rischio per determinare la necessità di adeguare le misure al variare delle minacce e degli impatti per l'interessato



https://www.osservatori.net/it_it/pubblicazioni/linea-guida-per-la-data-protection-impact-assessment

GRAZIE

Domande?

Luca Bechelli

Direttivo e Comitato Tecnico Scientifico Clusit

luca@bechelli.net
www.bechelli.net
https://twitter.com/luca_bechelli
https://www.facebook.com/bechelli.luca
http://www.linkedin.com/in/lucabechelli