Ordine dei Dottori Commercialisti e degli Esperti Contabili di Torino

ORDINE DEGLI AVVOCATI DI TORINO

ORDINE DEGLI INGEGNERI DELLA PROVINCIA DI TORINO

Tavolo di lavoro congiunto "Protezione dei dati personali – GDPR

Data breach: prevenire è meglio che curare

Esempi di data breach

a cura del Referente del TdL congiunto «Protezione dei dati personali – GDPR»
Ordine Ingegneri di Torino

Paolo Traversa *Ingegnere*

Torino, 14 maggio 2021

TaxLawPlanet™

Data breach nel mondo reale

DDAY.it

Grave falla nel sito del Ministero del Lavoro: i dati di tutti i dipendenti italiani in smartworking erano liberamente scaricabili

di Roberto Pezzali - 03/05/2021 12:19

Databreach
Ransomware
Senza backup
con backup e senza exfiltration in ospedale
Con backup
senza backup e con exfiltration
Mispostal
Errore invio di corrispondenza
Errore invio dati personali
Errore invio dati particolari
Data exfiltration
Dati di una candidature da sito web
Password da sito web
Credential stuffing
Lost or stolen device and paper doc
Furto di materiale cifrato
Furto di materiale non cifrato
furto materiale cartaceo
Internal human risk source
accesso di ex dipendente
trasmissione involontaria di dati a terza parte fidata
Social Engineering
Furto d'identità
Furto email

Ransomware

Caso	Dati Particolari	No risk	Risk	High risk	Motivo
Con backup e senza exfiltration	No	✓	X	X	Nessun rischio evidente
Senza backup (tempi lunghi di ripristino)	No	✓	✓	X	Rischio possibile
Con backup e senza exfiltration in ospedale	Sì	✓	✓	✓	Rischio alto
Senza backup e con exfiltration	No	✓	✓	✓	

Livello	Implicazioni
No Risk	Nessuna comunicazione richiesta, sola registrazione
Risk	Comunicazione all'autorità Garante
High risk	Comunicazione anche agli interessati

Data exfiltration

Caso	Dati Particolari	No risk	Risk	High risk	Motivo
Dati di una candidature da sito web	Sì	✓	✓	✓	
Password da sito web	No	✓	X	X	
Attacco sulle credenziali per un sito bancario (credential stuffing)	Sì	✓	✓	✓	

Internal human risk source

Caso	Dati Particolari	No risk	Risk	High risk	Motivo
Exfiltration di dati da parte di un ex-dipendente	No	✓	✓	X	
Trasmissione non voluta di dati ad una terza parte fidata	No	✓	X	X	

Lost or stolen devices and paper documents

Caso	Dati Particolari	No risk	Risk	High risk	Motivo
Furto di materiale contentente dati cifrati	No	✓	X	X	
Furto di materiale contenente dati non cifrati	Sì	✓	✓	✓	
Furto di documenti cartacei con dati personali particolari	Sì	✓	✓	✓	

Mispostal

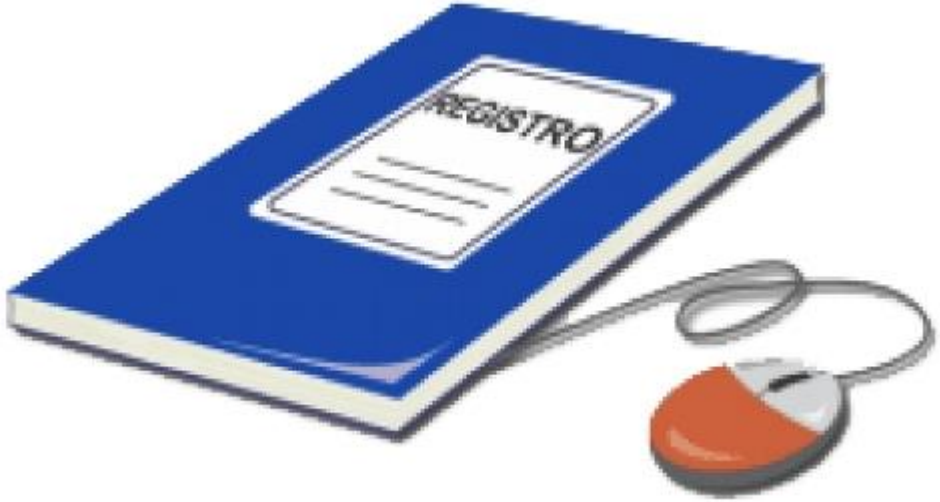
Caso	Dati Particolari	No risk	Risk	High risk	Motivo
Errore di invio di corrispondenza	No	✓	X	X	
Dati personali particolari inviati per errore	Sì	✓	✓	✓	
Dati personali inviati per errore	Sì	✓	X	X	
Errore di invio di corrispondenza	No	✓	✓	X	

Social engineering

Caso	Dati Particolari	No risk	Risk	High risk	Motivo
Identity theft	No	✓	✓	✓	
Email exfiltration	No	✓	✓	✓	

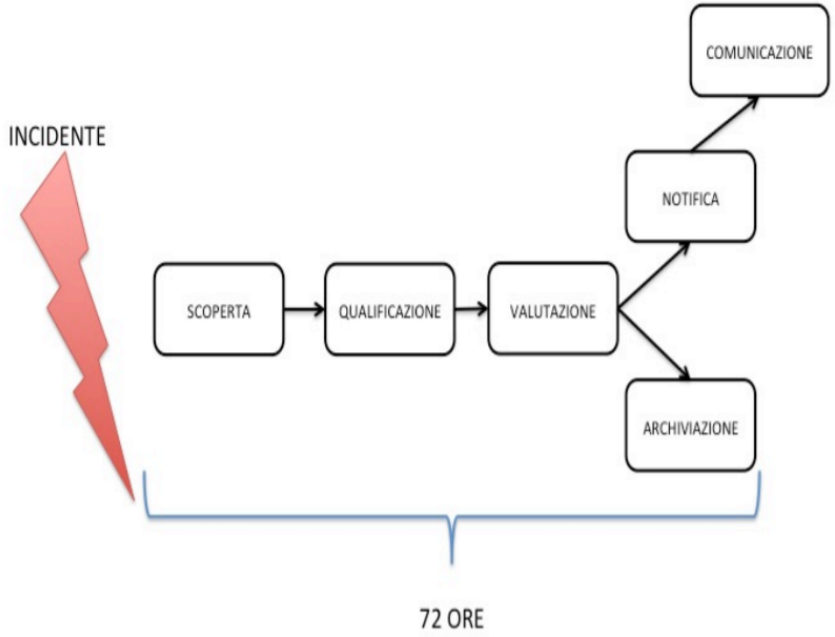
Contromisure

- Backup
- Cifratura
- Controllo identità
- Patch
- Antimalware
- Education
- Controllo attività cloud



Registro data breach: contenuti

- data e ora della violazione;
- natura della violazione;
- categorie di interessati coinvolte;
- categorie di dati personali coinvolte;
- effetti della violazione;
- contromisure adottate;
- se sia stata effettuata notifica all'Autorità Garante;
- se sia stata effettuata comunicazione agli interessati



Procedura di gestione databreach

Gestione della violazione

- Rilevazione e segnalazione
- Raccolta e analisi informazioni
- Notifica all'Autorità Garante (se necessaria)
- Notifica agli interessati (se necessaria)
- Documentazione

Valutazione della gravità

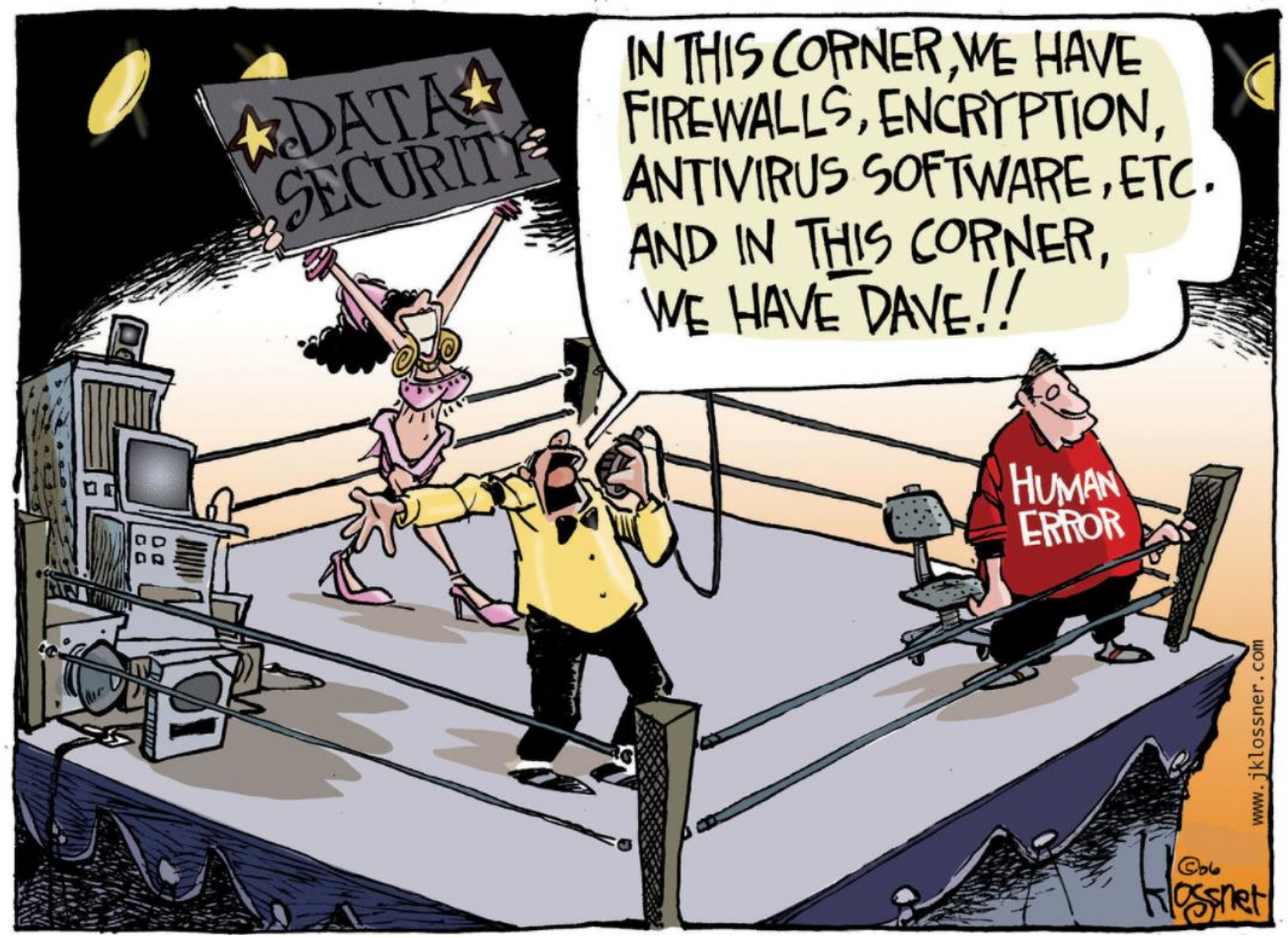
Template per la comunicazione

Template per la valutazione del rischio

E comunque…

- Ordinanza ingiunzione nei confronti di Agenzia regionale protezione ambientale Campania (ARPAC) - 14 gennaio 2021 [9538748]
  - Furto di un hard disk (denunciato e segnalato all'Autorità Garante)
  - Sanzione per «non aver adottato misure tecniche e organizzative adeguate per assicurare la protezione da trattamenti non autorizzati o illeciti o dalla perdita, e per garantire un livello di sicurezza adeguato al rischio, in violazione degli artt. 5, par. 1, lett. f), e 32 del Regolamento.» (sanzione 8.000 euro)

E comunque…



copyright 2006 John Klossner www.jklossner.com