SECURITY SUMMIT

Verona, 10 ottobre 2023

Security Summit

Clusit Associazione Italiana per la Sicurezza Informatica

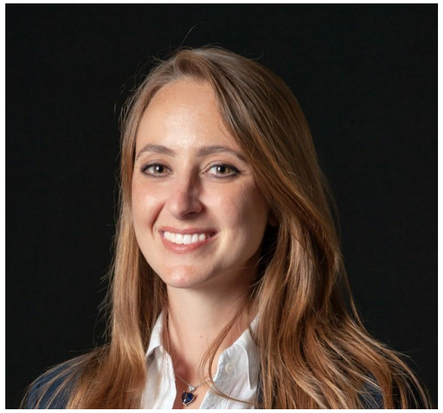
ASTREA Advanced Security, Training Research, Events Agency

Le responsabilità del management alla luce delle nuove normative in materia di cybersecurity

Lucrezia Falciai, Associate, Chiomenti

10 ottobre 2023 orario 15.40-16.20

Lucrezia Falciai

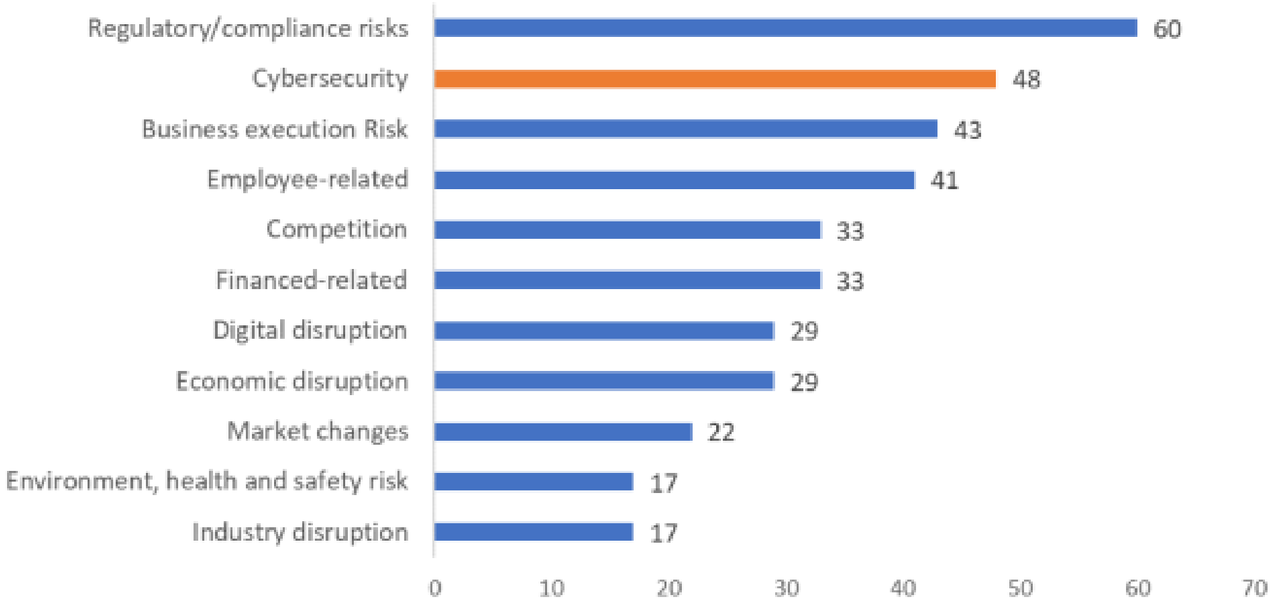


ASSOCIATE

La cybersecurity come elemento della corporate governance

- Cosa si intende per corporate governance
- Come la cybersecurity può contribuire alla corporate governance
- Approccio olistico

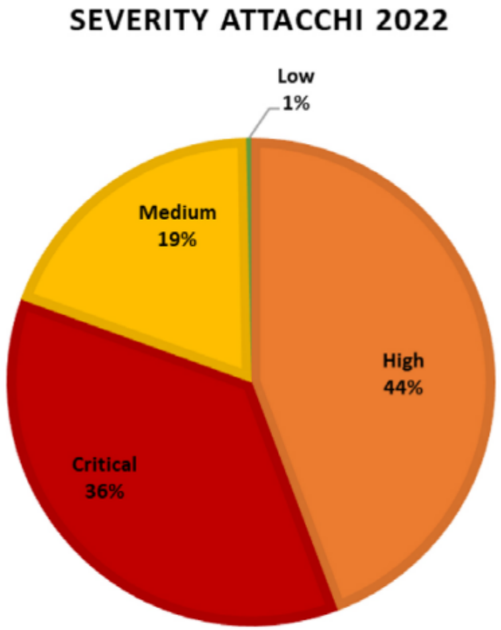
La cybersecurity come elemento della corporate governance



La cybersecurity come elemento della corporate governance

Attacchi infrastrutture critiche ad istituzioni, aziende e privati	2021	2022*	Variazione percentuale
Attacchi rilevati	5.434	12.947	+138%
Persone indagate	187	332	+78%

La cybersecurity come elemento della corporate governance



© Clusit - Rapporto 2023 sulla Sicurezza ICT in Italia

Le normative in materia di cybersecurity e il ruolo del management

Perimetro di Sicurezza Nazionale Cibernetica	Regolamento DORA	Direttiva NIS 2
Italia	Europa	Europa
Soggetti «critici» per la sicurezza nazionale	Entità finanziarie	Soggetti essenziali o importanti (es. energetico, trasporti, bancario, ma anche servizi postali, imprese alimentari, automotive, dispositivi medici)

Il Perimetro di Sicurezza Nazionale Cibernetica

Introduce:

- Reati 231
  - **fornisce** informazioni, dati o elementi di fatto non rispondenti al vero
  - **omette** di comunicare entro i termini prescritti i predetti dati, informazioni o elementi di fatto
  - **allo scopo di** ostacolare o condizionare l'espletamento dei procedimenti relativi alla comunicazione dell'elenco dei beni IT e della relativa architettura, la procedura del CVCN, le attività ispettive e di vigilanza
  - reclusione da 1 a 3 anni
- Sanzioni accessorie
  - incapacità ad assumere incarichi di direzione, amministrazione e controllo nelle persone giuridiche e nelle imprese, per un periodo di 3 anni a decorrere dalla data di accertamento della violazione
- Il controllo ID.AM-6
  - Nomina di un incaricato (es. Chief Information Security Officer – CISO)
    - ✓ Canale di comunicazione aperto

Il Regolamento DORA

- Quadro **di gestione e di controllo** interno. L'organo di gestione:
  - **assume la responsabilità finale** per la gestione dei rischi informatici dell'entità finanziaria;
  - **predispone** politiche miranti a garantire il mantenimento di standard elevati di disponibilità, autenticità, integrità e riservatezza dei dati;
  - **definisce chiaramente ruoli e responsabilità** per tutte le funzioni connesse alle TIC e **stabilisce adeguati meccanismi di governance** al fine di garantire una comunicazione, una cooperazione e un coordinamento efficaci e tempestivi tra tali funzioni;
  - ha la **responsabilità generale di definire e approvare** la strategia di resilienza operativa digitale compresa la **determinazione del livello appropriato di tolleranza per i rischi**;
  - **approva, supervisiona e riesamina** periodicamente **l'attuazione della politica di continuità operativa** delle TIC e **dei piani di risposta** e **ripristino** relativi alle TIC dell'entità finanziaria;
  - approva e riesamina periodicamente **i piani interni di audit** in materia di TIC dell'entità finanziaria, **gli audit** in materia di TIC e le più importanti modifiche a essi apportate;
  - assegna e riesamina periodicamente **le risorse finanziarie adeguate** per soddisfare le esigenze di resilienza operativa digitale dell'entità finanziaria rispetto a tutti i tipi di risorse, compresi i pertinenti **programmi di sensibilizzazione** sulla sicurezza delle TIC e le attività di **formazione** sulla resilienza operativa digitale, nonché le competenze in materia di TIC per tutto il personale;
  - approva e riesamina periodicamente la politica dell'entità finanziaria relativa alle **modalità per l'uso dei servizi TIC** prestati dal fornitore terzo di servizi TIC;
  - istituisce a livello aziendale **canali di comunicazione** che gli consentono di essere debitamente informato in merito a quanto segue:
    i. gli **accordi conclusi** con i fornitori terzi di servizi TIC sull'uso di tali servizi;
    ii. le relative eventuali **modifiche importanti e pertinenti** previste riguardo ai fornitori terzi di servizi TIC;
    iii. il **potenziale impatto** di tali modiche sulle funzioni essenziali o importanti soggette agli accordi in questione, compresa una sintesi dell'analisi del rischio per valutare l'impatto di tali modifiche, nonché almeno **i gravi incidenti TIC** e il loro **impatto**, le misure di risposta e ripristino e le misure correttive.

Il Regolamento DORA

- Quadro per la gestione dei rischi informatici
  - comprende almeno **strategie**, **politiche**, **procedure**, **protocolli** e **strumenti** in materia di TIC necessari per **proteggere debitamente e adeguatamente** tutti i patrimoni informativi e i risorse TIC, compresi software, hardware e server, nonché tutte le pertinenti infrastrutture e **componenti fisiche**, quali i locali, i centri di elaborazione dati e le aree designate come sensibili, così da garantire che tutti i patrimoni informativi e i risorse TIC siano **adeguatamente protetti contro i rischi**, compresi i danneggiamenti e l'accesso o l'uso non autorizzati;
  - è documentato e **riesaminato almeno una volta all'anno**, nonché in occasione di **gravi incidenti TIC** e in seguito a indicazioni o conclusioni delle autorità di vigilanza formulate a seguito di pertinenti test di resilienza operativa digitale o di processi di audit;
  - è periodicamente sottoposto ad audit
  - comprende una strategia di resilienza digitale che include metodi per affrontare i rischi

La Direttiva NIS 2

- L’organo di gestione **approva le misure di gestione dei rischi** di cybersecurity e sovraintende alla loro attuazione e può essere ritenuto **responsabile per la violazione**
- Adozione di misure **tecniche**, **operative** e **organizzative**
- Misure **adeguate e proporzionate** per gestire i rischi, **prevenire e ridurre al minimo** l’impatto degli incidenti per i **destinatari** dei servizi e per **altri servizi** connessi e/o interconnessi
- Gestione degli **incidenti**, sicurezza della **catena di approvvigionamento**, efficacia della **gestione dei rischi di cybersecurity**

Gli obblighi di formazione

- Il Perimetro di Sicurezza Nazionale Cibernetica
- Il Regolamento DORA
- La Direttiva NIS 2

La figura del Chief Information Security Officer – CISO

- Che ruolo può svolgere
- Come può supportare i processi di compliance
- In che termini deve essere coinvolto

Q&A