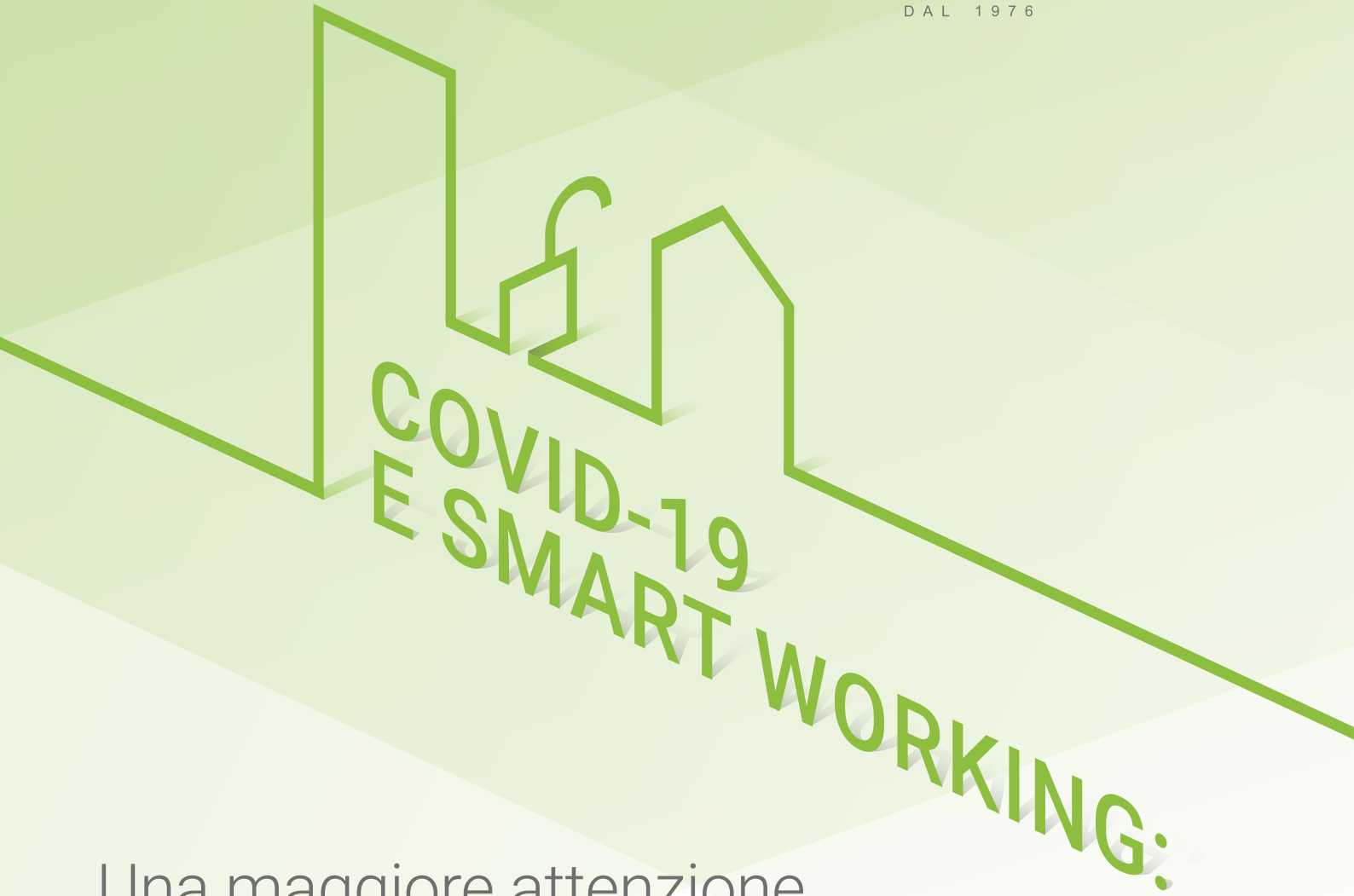
ANDREA SCAGLIARINI S.P.A.
BROKER DI ASSICURAZIONI
DAL 1976



# COVID-19 E SMART WORKING:

## Una maggiore attenzione alla Cyber Security aziendale

Nelle ultime settimane le misure d'urgenza messe in atto dal Governo per far fronte **all'emergenza Covid-19** hanno indotto numerose aziende ad adottare modelli di **Smart Working** così da evitare il blocco delle attività e le relative conseguenze.

Se questi modelli producono chiari benefici per società e lavoratori, è altrettanto vero che possono generare nuove **minacce alla sicurezza informatica aziendale** ed **estendere le superfici di attacco**.

Per garantire la Cyber Security servono ulteriori strumenti di gestione e riduzione dei rischi, sia lato azienda che lato dipendenti.

Aprile 2020


# Alcuni accorgimenti per migliorare la gestione del rischio Cyber in operatività da remoto.

- Scelta del modello per la fruizione dello Smart Working:
  BYOD – Bring Your Own Device,
  CYOD – Choose Your Own Device,
  COPE – Corporate Owned, Personally Enabled.
  L'accesso alla rete aziendale deve essere consentito ai soli device di cui l'azienda ha piena visibilità.
  Se è ammesso il BYOD, risulta determinante formalizzare policy interne a garanzia dell'integrità, affidabilità e sicurezza dei dati aziendali cui lo Smart Worker ha accesso, tramite controlli sui sistemi di sicurezza e prevenzione dei propri device (antivirus, firewall, security patch, etc);

- VPN – Virtual Private Network sicure e il pericolo delle fake VPN.
  Molti software VPN vengono distribuiti al solo scopo di ottenere fraudolentemente dati, tracciare i comportamenti degli ignari utilizzatori o sfruttare la larghezza di banda del device infettato per scopi il più delle volte illeciti.
  Una fake VPN potrebbe anche non applicare protocolli di crittografia al traffico dati, esponendo l'azienda a notevoli pericoli di divulgazione di informazioni riservate.
  Sarà pertanto necessario valutare attentamente il VPN service provider, la tipologia di protocollo di crittografia utilizzato e le review elaborate da altri utenti;

- Priviledged Access Management per l'accesso remoto ad asset digitali aziendali specifici, così da ridurre drasticamente il rischio di sottrazione di informazioni riservate;

- Back-up estesi ai device portatili in cui siano conservati dati aziendali, anche in Cloud per mitigarne il rischio di perdita;

- Aggiornamento dell'Incident Response Plan alla situazione attuale di operatività dell'azienda da remoto;

- Organizzazione di sessioni - in remoto - di Phishing Training per i dipendenti, al fine di riconoscere più facilmente i tentativi malevoli di sottrazione di dati.


# Best practice in tema di accesso remoto per mitigare il rischio di Cyber Incident.

- Utilizzo di connessioni internet sicure per l'accesso alla rete aziendale.
  Evitare l'uso di connessioni internet non protette da password, che potrebbero esporre i dati e gli asset digitali dell'azienda a numerose minacce;
- Adottare protocolli di crittografia per le informazioni gestite e conservate sui propri device - c.d. Encryption in transit ed Encryption at rest;
- Maggiore attenzione ai tentativi di Phishing legati all'emergenza Covid-19.

---

Nella corretta e completa filiera di gestione del Cyber Risk, acquista un ruolo sempre più importante il **trasferimento del rischio residuo** al mercato assicurativo, attraverso la sottoscrizione di **polizze Cyber & Privacy**.

La copertura offerta da tali polizze va a ricomprendere:

- **Spese di Incident Response** in caso di evento cyber / violazione dei dati e delle informazioni dell'azienda: consulenza IT, legale, tutela dell'immagine e della reputazione commerciale, consulenza in ambito estorsione informatica;
- **Interruzione attività** conseguente a **failure dei sistemi IT / attacco hacker**;
- **Responsabilità verso terzi per Data Breach.**

Siamo a vostra disposizione per approfondire l'argomento. Potete contattarci scrivendo all'indirizzo:

**cyber@scagliarinibroker.it**

Con i migliori saluti.

**Aprile 2020**

ANDREA SCAGLIARINI S.P.A.
BROKER DI ASSICURAZIONI
DAL 1976