

# Cyber Security e Data Protection fattori chiave per la Business Resilience

**CIONET**

CYBERSECURITY & BUSINESS RESILIENCE  
IN THE NEXT NORMAL

18 Febbraio 2021



# Digital Transformation

Il Cambiamento è già in atto

Una rivoluzione fatta di **soluzioni più efficienti**, **processi più agili** e **business più competitivi**, che richiede una mentalità aziendale nuova e più ampia, oltre all'adozione di tecnologie innovative.





## Agenda

- ❑ **NEW NORMAL- il mondo «dopo» il COVID-19**
- ❑ **BUSINESS RESILIENCE - «immunizzare» il Business**
- ❑ **CYBER SECURITY e DATA PROTECTION**
- ❑ **FOCUS**



**Paolo Asioli**

BU Manager  
Security & Compliance

# NEW NORMAL- il mondo «dopo» il COVID-19

- Dall'inizio della pandemia è esploso lo **Smart Working**
  - Aumento esponenziale della «**superficie di attacco**» delle aziende
  - Un **cambio di paradigma**, non si tornerà indietro
- **Crescita dei Cyber Attack** ben oltre il trend già consolidato negli ultimi anni
  - Aumento **da 5.000** attacchi/settimana a febbraio 2020 **fino a 200.000** attacchi/settimana ad aprile 2020
  - **Cyber Warfare** a livello internazionale – **Compromissione di credenziali privilegiate (Solarwinds!!!)**
  - **Cyber Crime** organizzato – **Attacchi a «duplice estorsione»**



# BUSINESS RESILIENCE – «immunizzare» il Business

- Rendere il **Business** «immune» agli attacchi Cyber
  - La **Business Continuity** deve essere allineata alla **Cyber Security** (backup e disaster recovery strumenti di ripartenza sicura)
  - La Cyber Security deve essere **intrinseca** a qualsiasi piano di Business Continuity (rif. ISO 27001 A.17)
- Adottare un approccio «**risk based**» alla Cyber Security (Gartner)
  - Valutare correttamente le **minacce**
  - Porre in atto contromisure **tecniche** ed **organizzative adeguate**
  - **Monitorare** il perimetro in modo da poter rispondere efficacemente alle minacce in modo sia *proattivo* che *reattivo* (fino all'**iperautomazione**)
- Cyber Security e Data Protection «**by design**» come strumento essenziale per «immunizzare» il Business



# CYBER SECURITY e DATA PROTECTION

- ❑ **Coordinare la Cyber Security** mediante un framework adeguato di **Compliance**
  - Senza un opportuno coordinamento (policy, processi) la Cyber Security rischia di essere un **esercito senza generale**
  - I framework di riferimento (NIST, ISO 27001) possono aiutarci a **organizzare** correttamente la «macchina da guerra» della Cyber Security (serve un «**Sistema di Gestione**» per garantire la **Sicurezza delle Informazioni**)
- ❑ La **normativa cogente (GDPR)** è sicuramente sprone e stimolo per intraprendere un percorso virtuoso
  - La **ISO 27701**, pubblicata nel 2019, è un ottimo riferimento per integrare la **Protezione dei Dati Personali** nei **Sistemi di Gestione della Sicurezza delle Informazioni** secondo la norma **ISO 27001**
  - Non è necessario raggiungere la certificazione ISO 27001 per beneficiare di un sistema di gestione allineato alla norma (di fatto guida esaustiva alle «best practice» indispensabili)



# FOCUS

- ❑ Cyber security e Information Security **Awareness** – *Lo Scudo Umano*
  - Il fattore umano deve passare da **debolezza** a **prima linea di difesa** dell'organizzazione



- ❑ Proteggere gli **endpoint**
  - I dispositivi, sempre più usati anche in **mobilità**, sono un «sorvegliato speciale» (**patching**, gestione dei **privilegi amministrativi**, **application control**, **remote control & assistance**) → **iperautomazione**

- ❑ Mettere in sicurezza le **utenze privilegiate**
  - ❑ Le utenze privilegiate (*amministratori di sistema, utenze di servizio*, ma anche credenziali di accesso remoto VPN) sono tra i **primi punti di attacco Cyber** (es. Solarwinds, Citrix, **Oldsmar water plant !!!**) sia dall'esterno che dall'interno



- ❑ La sicurezza nelle **reti di fabbrica** – *OT Security*

«**La S di OT sta per Security**» (cit. **Matteo Flora**) – Le reti OT sono delicate ma sempre più connesse, spesso caratterizzate da dispositivi obsoleti e non aggiornabili (**monitoraggio**)

Who, How, Where

**Paolo Asioli**

BU Manager  
Security & Compliance

[paolo.asioli@consoft.it](mailto:paolo.asioli@consoft.it)

Mob. +39 345 4560233

## **Consoft Sistemi S.p.a.**

**Torino**

via Pio VII, 127  
10127 TORINO - Italy  
Tel. +39 0113161571

**Roma**

Via G. Severano, 26  
00161 ROMA - Italy  
Tel. +39 06 51530032

**Milano**

Via Candiani, 73  
20158 MILANO - Italy  
Tel. +39 02 48022861

**Genova**

Via Pammatone, 7/34  
16121 Genova - Italy  
Tel. +39 013015525