INSTITUTO FEDERAL DE TELECOMUNICACIONES

Seminario Ciberseguridad: Retos y Oportunidades
14 y 15 de octubre de 2020

Tecnológico de Monterrey

# COVID-19 IMPACT ON CYBERSECURITY

# The COVID-19 impact on the global cybersecurity

Increasing focus on **securing remote infrastructure** and **IP** of enterprises due to **work from home** and **remote services** programs is leading to a market growth for cybersecurity.

Focus on cybersecurity as a **key business imperative** and not just as a support function is a refreshing change.

The cybersecurity spending in Technology, Media and Telecommunications sector is expected to increase.

Transition to remote work, though carried out rapidly and under intense pressure, has been broadly successful.

- Investments in technology infrastructure and people paid off
- Leaders and staff showed great resilience
- Accelerated digital transformation journeys continued
- Contrary to earlier expectations, productivity did not generally decline, and by some estimates it actually increased



# Rapidly implemented response to the COVID-19 pandemic, has opened new security risks.

## Remote work and staffing or availability disruption

- Greater remote access demands tested VPN bandwidth and network controls
- Some technology implementations had to be fast-tracked
- New requirement to secure and monitor home networks
- Personnel availability is affected

- *Are your remote access controls built to scale?*
- *How will security keep up with expedited tech projects and new support needs and changing landscape?*

## Increase in Ransomware and social engineering

- Increase in socially engineered cyber attacks target financial and sensitive data
- Phishing and malware attacks raise cyber risk levels
- Spread of misinformation poses crisis response challenges beyond technology

- *How is training and awareness keeping up with the need for agile threat detection and response to promote proactive identification of malicious activity?*

## Implicit risks from third parties

- Supply chain disruption present a new risk
- Third party providers may not be able to provide the same security coverage, increasing risks
- Configuration management for cloud providers

- *How are you assessing the impact of third party risks*
- *Are you continuously managing the security configurations of the cloud services*

Time to Reassess Your Risk Assessment

Agile & dynamic approach to critical information asset protection

- Control of physical and digital assets
- Visibility across endpoints
- Access Management
- Network segmentation
- Critical information protection
- Insider threats

Third-party risks including risks associated with cloud services