Due to COVID-19, many in the workforce are now mandated to work from home. This has wreaked havoc on both business leaders and individual employees. Both share responsibility in ensuring that cyber-attacks do not upset their already disrupted work environment.

Cyber criminals are taking advantage of the newly remote workforce as many do not have the same security on their home networks as their corporate environment. Additionally, many organizations haven’t deployed the right technologies or corporate security policies to ensure that all corporate-owned or corporate-managed devices have the exact same security protections implemented – regardless of whether they’re connected to an enterprise network or an open home Wi-Fi network.

During this critical time, IntraSystems can help you manage the security risk in the new work environment; leverage new policies and technologies; and empower your employees to work in a secure and productive environment. Below are some key recommendations for you to consider:

- **Understand the threats to your organization** | IntraSystems can assist your security team to identify likely attack vectors due to more employees working from home and prioritize the protection of their most sensitive information and business-critical applications.

- **Provide clear guidance and encourage communication** | IntraSystems can assist in implementing home-working policies to ensure your employees make their home-working environment secure. This includes instructing employees to communicate with internal security teams about any suspicious activities.

- **Provide the right security capabilities** | IntraSystems has the solutions to ensure all corporate-owned or managed devices are equipped with essential security capabilities, extending the same network security best practices that exist within the enterprise to all remote environments. These critical capabilities include:
  - An ability to securely connect users to their business-critical cloud and on-premise applications, such as video teleconferencing applications increasingly relevant for remote work environments
  - Endpoint protection on all laptops and mobile devices, including VPN tools with encryption
  - An ability to enforce multi-factor authentication (MFA)
  - An ability to block exploits, malware and command-and-control (C2) traffic using real-time, automated threat intelligence
  - An ability to filter malicious domain URLs and perform Blackhole DNS to prevent common phishing attacks