COSMOS
Navigate the Compliance Universe

CEP Magazine - July 2019
Non-corporate VPNs could be a virtual privacy nightmare

By Justin Jett

Justin Jett (justin.jett@plixer.com) is Director of Audit and Compliance for Plixer in Kennebunk, Maine, USA.

In the ever-connected digital world, virtual private networks (VPNs) facilitate working remotely, because they let users send all of their network traffic to the physical network of their organization without needing to be physically present. VPNs are inherently secure, because the traffic is encrypted from the individual's device to the organization's network. This gives businesses an extra layer of security for their remote employees, because they can be certain that any communication from business devices is being sent through the secure business network. Business resources are safely kept on the internal network, and only users connected to the VPN can access them.

From a consumer perspective, a VPN is a major privacy tool. Anyone can connect to a VPN service and effectively *hide* what they are doing from their ISP (or the ISP of the local coffee shop). When it comes to confidential information, such as banking or health details, a VPN is an important tool, because it prevents the person sniffing traffic at the local coffee shop from being able to intercept any of this information. This can come at a price, however.