5 Elements of a Cyber-Secure BYOD Policy

Personal laptops, tablets and smartphones are commonly used for work both inside and outside the office. As enterprise mobility becomes the norm, many small businesses will need to create bring-your-own-device (BYOD) policies to protect corporate data.

A BYOD policy that promotes small business cybersecurity will address five core elements:

1. An acceptable-use policy:

Specify ***who*** can access ***which*** corporate applications through a personal device; govern ***when***, ***where*** and ***how*** those apps can be used and ***what*** data they can access.

2. Data segregation:

Store all **corporate data remotely in a secure server** accessible either on the corporate network or through a **virtual private network (VPN)**; only personal data should be stored locally on a BYOD endpoint.

3. Data access:

Prohibit **non-sanctioned, consumer-grade apps** from accessing corporate data. Also known as "shadow IT," employees who use unapproved apps for work **put data at risk of a security breach.**

4. Authentication and user sessions:

Require authentication for each user login to corporate apps; **regulate password length**, **complexity and frequency** for changing them; automatically terminate remote user sessions after a certain period of inactivity.

5. MAM or MDM:

Use **mobile application management (MAM)** to control the corporate application (i.e. revoke account access if a BYOD device is lost or stolen). Alternatively, use **mobile device management (MDM)** to control the entire device (i.e. all data can be remotely wiped if the device is lost or stolen).

BYOD can act as a competitive advantage by promoting productivity and work flexibility for employees. Address the five high-level elements of a BYOD policy above to avoid introducing undue risk to your organization.

Comerica Bank®