BANC OF CALIFORNIA | TOGETHER **WE WIN**®

# THE LEADER'S CYBER READINESS GUIDE

## ESSENTIAL ELEMENTS OF A CULTURE OF CYBER READINESS

### You—The Leader

**Drive cybersecurity strategy, investment and cyber culture**

- Your awareness of the basic risks drives actions and activities that build and sustain a culture of cybersecurity.

### Your Staff—The Users

**Develop security awareness and vigilance**

- Your staff will often be your first line of defense. They should continuously grow the skills to practice and maintain readiness against cybersecurity risks.

### Your Systems—Operations

**Protect critical assets and applications**

- Information is the lifeblood of any business; it is often the most valuable of a business's intangible assets.
- Know where this information resides, know what applications and networks store and process that information, and build security into and around these.

### Your Surroundings—Digital Workspace

**Ensure that only those who belong on your digital workspace have access**

- Setting approved access to your digital environment controls who operates on your systems and with what level of authorization and accountability.

### Your Data—What the Business Is Built On

**Make backups and avoid the loss of information critical to operations**

- Even the best security measures can be circumvented. Learn to protect your information where it is stored, processed and transmitted.
- Have a contingency plan to recover systems, networks and data from known, accurate backups.

### Your Ability to Recover

**Limit damage and quicken restoration of normal operations**

- The strategy for responding to and recovering from compromise: Plan, prepare for and conduct drills for cyberattacks as you would for a fire.
- This requires having established procedures and plans and communicating during a crisis.

© 2025 Banc of California. All rights reserved. Member FDIC.