



**BANC OF
CALIFORNIA**

TOGETHER WE WIN®

THE IT PROFESSIONAL'S CYBER READINESS GUIDE



ESSENTIAL ACTIONS FOR BUILDING A CULTURE OF CYBER READINESS



Business Leader



Your Employees



Your Systems



Your Access



Your Data



**Your Actions Under
Stress**

BUSINESS LEADER



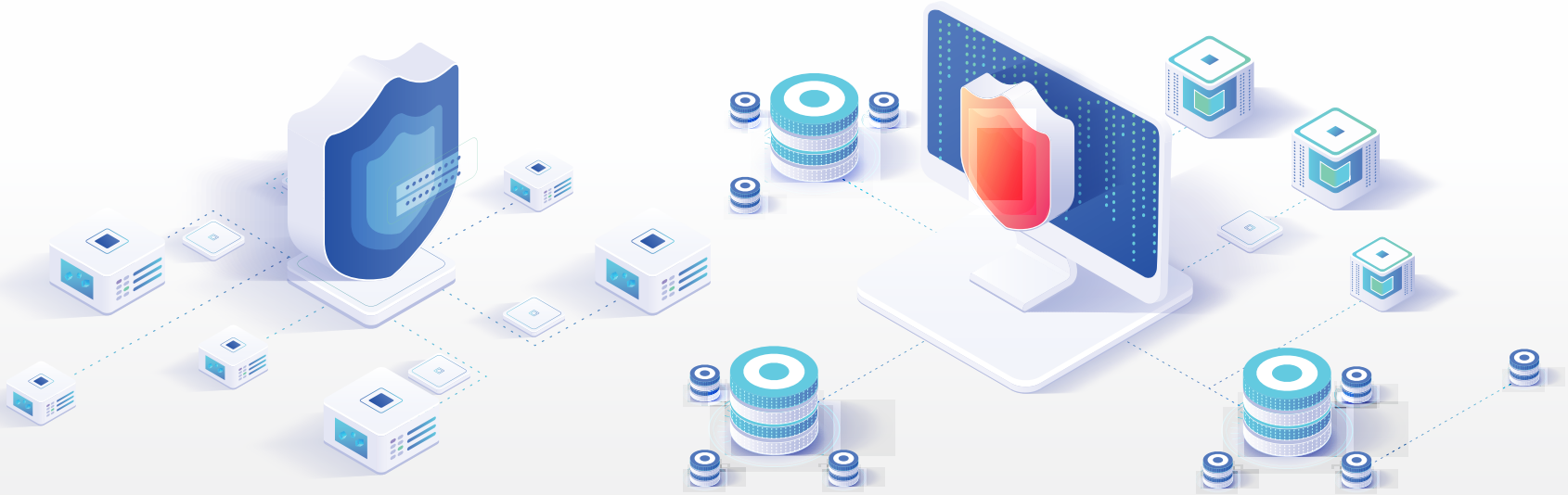
- ✓ Invest in cybersecurity.
- ✓ Review who is dependent on IT.
- ✓ Build a network of trusted relationships with sector partners and government agencies for access to timely cyber threat information.
- ✓ Acknowledge cybercrime as a business risk and be proactive.
- ✓ Develop cybersecurity policies.

YOUR EMPLOYEES



- ✓ Leverage basic cybersecurity training to understand cybersecurity concepts and implement best practices.
- ✓ Develop a culture of awareness to encourage employees to make good choices online.
- ✓ Learn about risks such as phishing and business email compromise.
- ✓ Identify available training resources through professional associations, academic institutions, private sector and government sources.
- ✓ Be aware of current events related to cybersecurity, using lessons learned and reported events to remain updated on the current threat environment.

YOUR SYSTEMS



- ✓ Learn what's on your network and maintain an inventory of hardware and software assets to know what is at risk from an attack.
- ✓ Leverage automatic updates for all operating systems and third-party software.
- ✓ Implement secure configurations for all hardware and software assets.
- ✓ Remove unauthorized hardware and software from systems.
- ✓ Leverage email and web browser security settings to protect against spoofed or modified emails and unsecured webpages.
- ✓ Create application integrity and whitelisting policies so only approved software is allowed on your systems.

YOUR ACCESS



- ✓ Learn who is on your network and maintain inventories of network connections (user accounts, vendors, business partners, etc.).
- ✓ Implement multifactor authentication for all users.
- ✓ Grant access and admin permissions based on a need-to-know basis and least privilege.
- ✓ Use unique passwords for all user accounts.
- ✓ Develop IT policies and procedures addressing changes in user status (transfers, termination, etc.).

YOUR DATA



- ✓ Know what information resides on your network. Maintain inventories of critical or sensitive information.
- ✓ Establish regular automated backups.
- ✓ Install malware protection capabilities.
- ✓ Manage network and perimeter components, host and device components, data at rest and in transit, and user behavior activities.

YOUR ACTIONS UNDER STRESS



- ✓ Develop an incident response and disaster recovery plan outlining roles and responsibilities. Test it often.
- ✓ Create a business impact assessment to prioritize resources and identify which systems must be recovered first.
- ✓ Create a call list of whom to call for help (outside partners, vendors, government/industry responders, technical advisors and law enforcement).
- ✓ Develop an internal reporting structure to detect, communicate and contain attacks.