Your success depends on Cyber Readiness. Both depend on YOU.

Managing cyber risks requires building a culture of cyber readiness.

**Essential Elements of a Culture of Cyber Readiness:**

**Yourself - The Leader**
- Drive cybersecurity strategy, investment, and culture

Your awareness of the basics drives cybersecurity to be a major part of your operational resilience strategy, and that strategy requires an investment of time and money. Your investment drives actions and activities that build and sustain a culture of cybersecurity.

**Your Surroundings - The Digital Workplace**
- Ensure only those who belong on your digital workplace have access

The authority and access you grant employees, managers, and customers into your digital environment needs limits, just as those set in the physical work environment do. Setting approved access privileges requires knowing who operates on your systems and with what level of authorization and accountability.

**Your Staff - The Users**
- Develop security awareness and vigilance

Your staff will often be your first line of defense, one that must have - and continuously grow - the skills to practice and maintain readiness against cybersecurity risks.

**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 with a patient, sophisticated adversary. Learn to protect your information where it is stored, processed, and transmitted.

Have a contingency plan, which generally starts with being able to recover systems, networks, and data from known, accurate backups.

**Your Systems - What Makes You Operational**
- Protect critical assets and applications

Information is the life-blood of any business; it is often the most valuable of a business' 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 Actions Under Stress**
- 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 a fire. Make your reaction to cyberattacks and system failures an extension of your other business contingency plans. This requires having established procedures, trained staff, and knowing how - and to whom - to communicate during a crisis.
Consistent with the NIST Cybersecurity Framework and other standards, these actions are the starting point to Cyber Readiness. To learn more, visit CISA.gov/Cyber-Essentials.