THE LEADER’S GUIDE

Reducing your organization's cyber risks requires a holistic approach - similar to the approach you would take to address other operational risks. As with other risks, cyber risks can threaten:

- Your ability to operate / Access Info
- Your reputation / Customer Trust
- Your bottom line
- Your organization's survival

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 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 resilience against cybersecurity risks.

**Your Systems** - What Makes You Operational

Protect critical assets and applications

Information is the lifeblood of any business; it is often the most valuable of a business' intangible assets.

Know where this information resides, know what applications and network areas process that information, and build security into and around these.

**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 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.

CISA.gov/Cyber-Essentials

For tech specs on building a Culture of Cyber Readiness, flip page →
<table>
<thead>
<tr>
<th>Organizations living the culture have:</th>
<th>Leverage basic cybersecurity training to improve exposure to cybersecurity concepts, terminology and activities associated with implementing cybersecurity best practices.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lead investment in basic cybersecurity.</td>
<td></td>
</tr>
<tr>
<td>Determined how much of their operations are dependent on IT.</td>
<td></td>
</tr>
<tr>
<td>Built a network of trusted relationships with sector partners and government agencies for access to timely cyber threat information.</td>
<td></td>
</tr>
<tr>
<td>Approached cyber as a business risk.</td>
<td></td>
</tr>
<tr>
<td>Lead development of cybersecurity policies.</td>
<td></td>
</tr>
</tbody>
</table>

**THE IT PROFESSIONAL’S GUIDE**

**Essential Actions for Building a Culture of Cyber Readiness:**

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

- **Your Staff**
  - Make cybersecurity awareness and vigilance

- **Your Systems**
  - Develop security awareness and applications

- **Your Surroundings**
  - Protect critical assets and applications

- **Your Data**
  - Make backups and avoid loss of info critical to operations

- **Your Actions Under Stress**
  - Improve resiliency against cyber incidents when stress is high

**Backup Data**

- Employ a backup solution that automatically and continuously backs up critical data and system configurations.

**Multi-Factor Authentication**

- Require multi-factor authentication (MFA) for accessing your systems whenever possible. MFA should be required of all users, but start with privileged, administrative and remote access users.

**Patch & Update Management**

- Enable automatic updates whenever possible. Replace unsupported operating systems, applications and hardware. Test and deploy patches quickly.