



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

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



Develop security awareness and vigilance

Your Data - What the Business is Built On

Make backups and avoid the loss of

information critical to operations



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



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

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.

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 Surroundings - The Digital Workplace

Ensure only those who belong on your digital workplace have access



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.

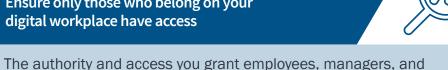




Limit damage and quicken restoration of normal operations

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.



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

customers into your digital environment needs limits, just as those

accountability.





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.



THE IT PROFESSIONAL'S GUIDE Actions for leaders. Since the provider of the pro

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



Yourself

Drive cybersecurity strategy. investment and culture

Organizations living the culture have:

- ✓ Lead investment in basic cybersecurity.
- Determined how much of their operations are dependent on IT.
- Built a network of trusted relationships with sector partners and government agencies for access to timely cyber threat information.
- Approached cyber as a business risk.
- Lead development of cybersecurity policies.



Your Staff

Develop security awareness and vigilance

Organizations living the culture have:

- Leveraged basic cybersecurity training to improve exposure to cybersecurity concepts, terminology and activities associated with implementing cybersecurity best practices.
- Developed a culture of awareness to encourage employees to make good choices online.
- Learned about risks like phishing and business email compromise.
- Identified available training resources through professional associations, academic institutions, private sector and government sources.
- Maintained awareness of current events related to cybersecurity, using lessonslearned and reported events to remain vigilant against the current threat environment and agile to cybersecurity trends.



Your Systems

Protect critical assets and applications

Organizations living the culture have:

- Learned what is on their network. Maintained inventories of hardware and software assets to know what is in-play and at-risk from attack.
- Leveraged automatic updates for all operating systems and third-party software.
- ✓ Implemented secure configurations for all hardware and software assets.
- Removed unsupported or unauthorized hardware and software from systems.
- Leveraged email and web browser security settings to protect against spoofed or modified emails and unsecured webpages.
- Created application integrity and whitelisting policies so that only approved software is allowed to load and operate on their systems.



Your Surroundings

Ensure only those who belong on your digital workplace have access

Organizations living the culture have:

- Learned who is on their network. Maintained inventories of network connections (user accounts, vendors, business partners, etc.).
- Leveraged multi-factor authentication for all users, starting with privileged, administrative and remote access users.
- Granted access and admin permissions based on need-to-know and least privilege.
- Leveraged unique passwords for all user accounts.
- Developed IT policies and procedures addressing changes in user status (transfers, termination, etc.).



Your Data

critical or sensitive

information.

protected.

Leveraged malware

offline copies.

activities.

protection capabilities.

Leveraged protections for

backups, including physical

security, encryption and

Learned what is happening

network and perimeter

on their network. Managed

components, host and device

components, data-at-rest and

in-transit, and user behavior

Make backups and avoid loss of info critical to operations



Your Actions Under Stress

Limit damage and quicken restoration of normal operations

Organizations living the culture have: Organizations living the culture have:

- Lead development of an incident response and disaster recovery plan outlining roles and responsibilities. Test it often.
- Established regular automated backups and assessments to prioritize redundancies of key systems. resources and identify which systems must be recovered Learned how their data is first.
 - Learned who to call for help (outside partners, vendors, government / industry responders, technical advisors and law enforcement).
 - Lead development of an detect, communicate and
 - Leveraged in-house containment measures to limit the impact of cyber



