

NEXT STEP: LEVEL UP YOUR DEFENSES

SECURING
THE NEXT
250

USE LOGGING ON YOUR SYSTEMS



Log system activity so your team can monitor signs of threat actors trying to access your systems.

BACK UP DATA



Incidents happen, but when you back up critical information, recovery is faster and less stressful. Put a backup plan in place to protect your systems and keep things running smoothly.

ENCRYPT DATA



Encrypting your data and devices strengthens your defense against attacks. Even if criminals gain access to your files, information stays locked and unreadable. Make encryption part of your security strategy.

TWO NEW ACTIONS FOR 2026

CPG 2.0 1.C

HAVE A INCIDENT RESPONSE PLAN AND USE IT!

Organizations should develop, maintain, update, and regularly exercise IR plans for common threat scenarios such as ransomware attacks. Ensure drills are realistic and include all relevant stakeholders, such as organizational leadership and legal counsel, in addition to technical personnel. IR plans should be reviewed and drilled on an annual basis at a minimum.



CPG 2.0 6.A

BE PREPARED FOR SYSTEM DISRUPTIONS

Organizations should develop and execute plans to recover and restore service to critical assets or systems that might be impacted by a cybersecurity incident. Consider including the ability to execute mission essential functions without access to critical assets or even internet access

(e.g., shift to paper-based operations, radio communications, etc.).



MORE WAYS TO
**STAY
SECURE**

GET A **.GOV DOMAIN** IF ELIGIBLE
Learn more at get.gov.

REPORT CYBER INCIDENTS TO CISA
Report incidents to CISA at cisa.gov/report.



**CYBERSECURITY
AWARENESS
MONTH**
OCTOBER 2026

cisa.gov/cybersecurity-awareness-month