BUILD YOUR RANSOMWARE PREPAREDNESS PLAN

1 ESTABLISH YOUR CRISIS TEAM

Your broad team should include your agency leadership, IT director, communications director, HR director, and other department heads

2 MAP OUT YOUR INFRASTRUCTURE

Review the criticality of your systems, applications, and data with stakeholders—and against compliance requirements

3 DEVELOP YOUR TECHNICAL RESPONSE

Document what you can shut down immediately, under what conditions you should shut down critical systems, and how you reconnect everything and in what order

4 ESTABLISH YOUR COMMUNICATIONS RESPONSE

Document the audiences that will require communications outreach —and craft canned messages that can be rapidly customized to speed your response time

5 PUT YOUR PLAN INTO PRACTICE

Implement regular tabletop exercises—ensuring vulnerabilities are addressed early and everyone is prepared to respond in the heat of the moment

arcserve®