Gauging Your Organization's Ransomware Readiness

Consider the following questions when developing a ransomware prevention and protection plan.

1. Does your organization have regularly scheduled backups?
   • Are these backups disconnected from your network, either via cloud storage systems or air-gapped USBs/hard drives?

2. Are any nonessential devices connected to your organization’s network?
   • Can they be moved to other networks that do not house sensitive data?

3. Does your organization understand the regulatory and legal risks involved with paying a ransom?
   • Legal guidance on this varies from country to country and is frequently updated.

4. Does your organization regularly update its software and systems? Are updates automated?

5. Does your organization have a plan for how to deal with a ransomware attack and the loss of valuable data?

6. Does your organization have a cyber insurance policy? If so, how does that plan cover ransomware attacks?
   • Some plans explicitly prohibit ransom payments, while others will cover such a payment as part of the policy.