Are you prepared for ransomware?

80%

of cybersecurity decision makers report their organization has engaged in ransomware-specific incident readiness activities.

Most ransomware (like WannaCry and Petya) is highly successful at rendering files inaccessible until a ransom is paid. Many organizations reserve funds to pay ransom, but this is a complicated decision and depends on a business risk analysis that many companies haven't engaged in. Respondents to a recent ESG survey stated they prepare for the worst with services like IBM's X-Force Incident Response and Intelligence Services, which offers a step-by-step guide in ransomware readiness. The first step is often end-user education, since most ransomware attacks target files commonly created and utilized by users.

Learn more

Original survey question:

Has your organization engaged in incident readiness activities specific to ransomware or destructive malware events to prepare and understand how to restore or rebuild your IT systems after such an event?

Survey respondents:

334 cybersecurity decision makers responsible for the policies, processes, or technical safeguards used for incident readiness and response at their organization.

ESG Research Survey, Incident Readiness Trends: Do Confidence Levels Match Preparation Efforts?, July 2019.

IBM