Ten steps to successful ransomware response

by John P. Carlin

1 ISOLATE THE INFECTED SYSTEMS

Immediately disconnect the infected systems from the network to prevent the ransomware from spreading. This can include disabling Wi-Fi, unplugging network cables and turning off Bluetooth.

2 SECURE BACKUPS

Backups are the most important resource for recovering from ransomware attacks, which is why many cybercriminals target backup files as well. To avoid this, ensure backup systems are fully disconnected from the network and restrict access to them until the incident is resolved.

3 ACTIVATE RESPONSE TEAM

Establish a regular cadence and communication channels for the core incident response team, including legal, IT, security, communications, business and external support.

4 ASSESS THE BUSINESS IMPACT

The scope of an incident's impact on business operations will influence the prioritization of all other response and recovery measures.

5 ESCALATE INTERNALLY

Based on the severity of the incident, timely escalate to executives and the board.

6 ENGAGE WITH LAW ENFORCEMENT

Law enforcement can provide indicators of compromise and additional information about particular ransomware variants to assist with your investigation and help secure your systems. In some cases, law enforcement may be able to provide decryption keys to help recover files, and they may be able to track down and recover any ransom paid.

7 ENGAGE EXTERNAL SUPPORT

Engage third-party experts as needed to assist with forensic investigation, negotiate with threat actors and facilitate any ransomware payments, support PR and crisis communications, analyze impacted data to identify affected individuals, and deliver required notifications.

8 DEVELOP AND INITIATE A RECOVERY STRATEGY

Evaluate the feasibility and practicality of using backups to restore your systems and data. If restoring from backup is not feasible or practical and a decryption key is not available, develop a strategy to negotiate with the threat actor and perform the necessary diligence to make any payment in compliance with sanctions and other applicable legal restrictions.

9 CONSIDER COMMUNICATIONS STRATEGY AND LEGAL OBLIGATIONS

Prepare and execute a strategy to communicate with your insurer, customers, employees, investors, other affected individuals and regulators — e.g., sector-specific regulators and state attorneys general — including assessments of statutory, regulatory, and contractual notification and disclosure obligations.

10 DOCUMENT THE INVESTIGATION AND LESSONS LEARNED

Consider whether to prepare a privileged report of the incident, response, remedial measures and resolution, as well as opportunities to improve the company's security posture and incident response procedures.

Published March 2025.

iapp.org