DIGITAL FORENSICS

INCIDENT HELP SHEET

Ransomware Incident

Overview

Ransomware response needs fast containment without destroying the evidence needed to understand entry, spread, persistence and data access.

Act quickly

If essential services, safety-critical systems or regulated data are affected, escalate immediately to the appropriate incident, legal and regulatory contacts.

What to do now

01 Isolate affected systems

Disconnect network access where safe, while avoiding unnecessary power-off of systems that may hold volatile evidence.

02 Preserve logs and alerts

Retain security alerts, firewall logs, identity logs, endpoint telemetry and ransom notes.

03 Record affected assets

List encrypted devices, servers, shares, cloud systems and user accounts.

04 Protect backups

Prevent compromised accounts or systems from reaching backup infrastructure.

05 Use a clean communications channel

Coordinate the response from unaffected systems and accounts.

06 Escalate appropriately

Engage incident response, legal, insurance and management contacts as required.

DIGITAL FORENSICS

INCIDENT HELP SHEET

Ransomware Incident

What not to do

- ! Do not mass-delete files or antivirus detections before evidence is recorded.
- ! Do not reconnect isolated machines simply to test whether they are usable.
- ! Do not restore backups into an environment that may still be compromised.
- ! Do not assume encryption is the only issue; data theft may also have occurred.

Evidence to preserve

- ✓ Ransom note and file extensions
- ✓ Security and endpoint alerts
- ✓ Authentication and VPN logs
- ✓ Firewall, proxy and DNS logs
- ✓ Suspicious files, scripts and scheduled tasks
- ✓ Timeline of first symptoms and containment actions
- ✓ List of affected and unaffected systems

Before speaking to a forensic specialist

Keep the original device or account available, avoid unnecessary changes, write down the sequence of events while it is fresh, and explain any containment or recovery actions already taken. The more complete the context, the easier it is to assess what evidence may still be available.

Need help now?

Digital Forensics can assist with evidence preservation, forensic examination and clear reporting.

Phone: 01634 672677
Email: info@digital-forensics.co.uk
Web: digital-forensics.co.uk