Preserving Evidence After A Cyber Attack Or Ransomware Incident

Understanding how to preserve evidence after a cyber attack or ransomware incident is crucial for UK litigators, in-house counsel, and investigators. This guide details the necessary steps to secure digital evidence, supporting legal and regulatory obligations while navigating business recovery challenges.

e-discovery.uk, Computer Forensics Lab. Published 2026-08-31.
https://e-discovery.uk/library/preserving-evidence-after-a-cyber-attack-or-ransomware-incident

INCIDENT EVIDENCE · A GUIDE FOR UK LAWYERS Preserving Evidence After a Cyber-Attack or Ransomware Incident Recovering the Business Without Destroying the Case COMPUTER FORENSICS LAB

§ ABOUT THE AUTHOR PREPARED BY COMPUTER FORENSICS LAB E-DISCOVERY TEAM ESTABLISHED 2007 · LONDON ISO 17025-ALIGNED PROCEDURES INCIDENT EVIDENCE PRESERVATION INTRUSION TIMELINE RECONSTRUCTION CPR PART 35 EXPERT REPORT S FULL CHAIN-OF-CUSTODY DOCUMENTATION

§ CONTENTS

§ 01 · ORIENTATION Executive summary THE HEADLINE POINT: PRESERVEBEFOREYOUREBUILD: IMAGES, VOLATILEDATAAND LOGSCAPTUREDINTHEFIRSTHOURSSERVEEVERYAUDIENCETHEINCIDENTCREATES: ANDTHERECOVERYTHATSKIPSPRESERVATIONANSWERSREGULATORS, INSURERSAND COURT S FROM MEMORY

§ 02 · FIRST PRINCIPLES The problem in plain English: recovery eats evidence

§ 03 · THE FIRST HOURS The first hours: what to preserve before anything is rebuilt

§ 04 · THEINTRUSION ' SSTORY The intrusion evidence map: entry, movement, exfiltration, impact

§ 05 · THECROWDEDBRIDGE Working with insurers, IR firms and the preservation gap

§ 06 · THECLOCKS The legal audiences and their clocks: ICO, regulators, subjects, courts

§ 07 · THELONGTAIL From incident to litigation: the uses the estate must support

§ 08 · THEWIDERMAP Source architecture: where else the evidence lives QUESTION

PLATFORM CLEARED / END POINT NETWORK SECURIT Y EXTERNAL LAYER LAYER TOOLING LAYER IDENTIT Y / ATTACKER- LOGS LOST

§ 09 · IN THE WILD Worked examples EXAMPLE1 · THE72 - HOURREPORTWRITTENFROMEVIDENCE EXAMPLE2 · THEREBUILDTHATERASEDTHESUPPLIERCLAIM EXAMPLE3 · THENEGATIVETHATWASWORTHPROVING

§ 10 · WHEREITGOESWRONG Common mistakes and technical limitations Common mistakes Technical limitations

§ 11 · INTERROGATORIES & DRAFTING AIDS Questions to ask · Suggested wording Ask your client (in the first hours) Ask the IR firm / insurer panel Ask third parties (suppliers, MSPs, providers) SUGGESTED WORDING · PRESERVATION M AN DATE FOR THEIR ENGAGEMENT

§ 12 · QUICK CONTROL Checklist and red flags · When to involve a digital forensic expert The incident-preservation checklist Red flags When to involve a digital forensic expert

§ 13 · COMMON QUESTIONS Frequently asked questions Won't preservation slow down our recovery when every hour of d own time costs money? Should we pay the ransom, and does forensics bear on it? How can we possibly know within 72 hours what data was affected? The attackers cleared the server logs. Is the investigation over? Our insurer's IR firm is handling everything. Do we need our own forensic adviser? Can we prove data was NOT taken?

§ 14 · REFERENCE Glossary Sources and authoritative references DISCLAIMER

§ HOW A SPECIALIST LABORATORY CAN ASSIST Working with Computer Forensics Lab Speak to a forensic examiner, not a salesperson. INSTRUCTTHELAB NEWENQUIRIESEMAILE - DISCOVERY

Questions and answers

Won't preservation slow down our recovery when every hour of d own time costs money?

Marginally and in parallel, not serially: imaging designated systems and export in g logs runs alongside containment, and the §3 order in g exists precisely to avoid gating the rebuild: hours of examiner work against Example 2's two-year alternative. The expensive version of preservation is the one attempted retrospectively.

Should we pay the ransom, and does forensics bear on it?

That is a legal-strategic decision taken under advice: sanctions screening on the attribution evidence, insurer position, data-recovery realities and leak-site risk all feed it: and the preserved artefacts (strain, communications, exfiltration analysis) are its factual inputs: Example 3's firm declined from an evidenced position. Forensics does not make the call; it makes the call informed.

How can we possibly know within 72 hours what data was affected?

Often only part i all y: which the regime anticipates: the initial report states what is assessed, staged supplementation follows the analysis, and the §3-preserved logs are what let the assessment converge quickly: Example 1's hour-60 answer. What the clock punishes is not incomplete knowledge but unassessed assertion.

The attackers cleared the server logs. Is the investigation over?

No: log-clearing is expected tradecraft and §8's whole design answers it: the network layer, identity provider, EDR telemetry, backup systems and external sources each hold independent copies of phases the attacker could not reach: and the clearing itself, documented per guide 110, is evidence. Single-source dependence is the vulnerability; the layered harvest is the cure.

Our insurer's IR firm is handling everything. Do we need our own forensic adviser?

For evidence, prudently yes: the panel's mandate is containment, recovery and the claim, and §5's preservation gap is structural, not a criticism: your adviser states the mandate, takes custody of the preserved estate, and serves the audiences the panel does not: supplier claims, subject-action defence, the eventual disclosure exercise. One estate, two mandates, both staffed.

Can we prove data was NOT taken?

Sometimes, and it is precious when possible: bounded egress volumes, bracketed access, absent staging progression and a silent leak site: Example 3's finding: supportable only where the network and platform layers were harvested in hour one. The negative cannot be reconstructed later: it is the single best argument for treating