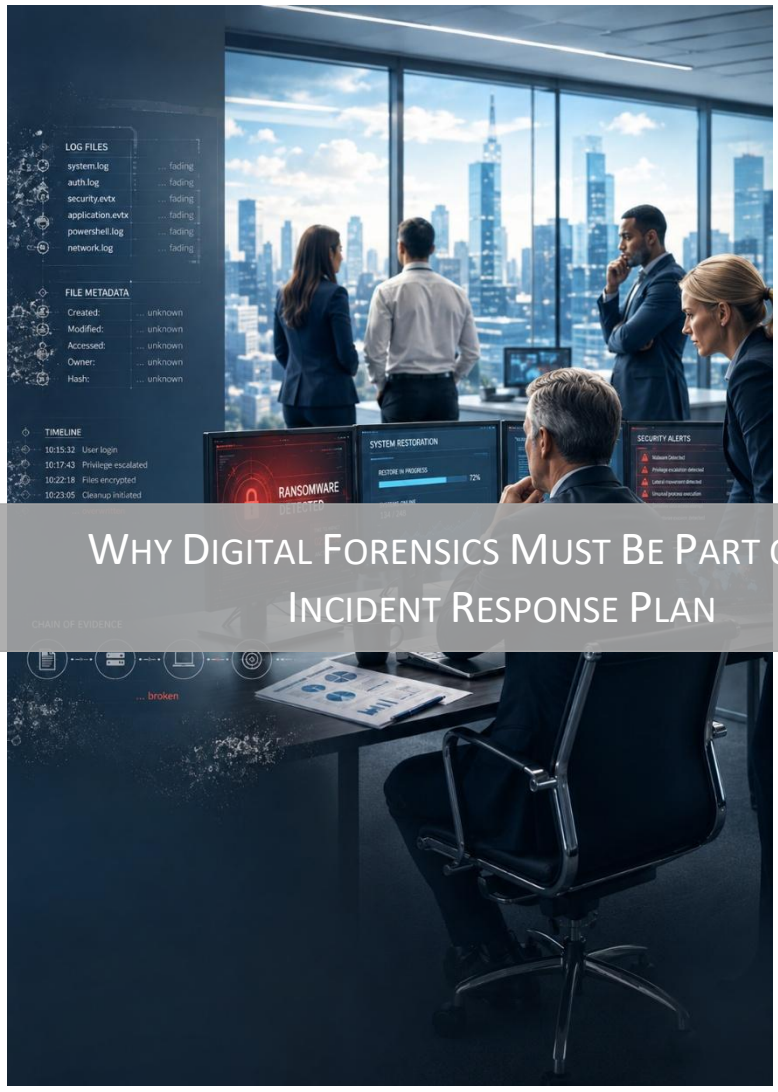

Why Digital Forensics Must Be Part of Your Incident Response Plan

Author – Andrew Smith

August 2026

Why Digital Forensics Must Be Part of Your Incident Response Plan

When a company suffers a ransomware attack or another serious cyber incident, the first instinct is usually to restore operations as quickly as possible.

Management wants systems brought back online. Employees need access to files and applications. Customers expect services to continue. The IT team is placed under immediate pressure to contain the problem, rebuild affected systems and return the business to normal.

Those actions are understandable and necessary. However, when recovery begins before a proper forensic investigation, the company may permanently lose the evidence needed to understand what actually happened.

By the time management realises that the internal IT team cannot answer the most important questions, critical evidence may already have been deleted, overwritten or destroyed.

IT Support and Digital Forensics Are Not the Same

Internal IT teams understand the company's systems better than almost anyone. They know how the network is configured, which applications are business-critical and how to restore services from backup.

However, maintaining and recovering systems is very different from conducting a digital forensic investigation.

After a ransomware attack, business leaders may need answers to questions such as:

- How did the attackers gain access?
- When did the intrusion begin?
- Which systems and accounts were compromised?
- Did the attackers move through the network?
- Was sensitive or personal information accessed or stolen?
- Is the attacker still present?
- Can restored systems be trusted?
- What evidence is available for insurers, regulators, customers or legal proceedings?

These questions cannot always be answered by reviewing a few system logs or asking the IT department what it observed during the attack.

A forensic investigation requires specialised tools, investigative methods and evidence-preservation procedures. It also requires an understanding of how attacker activity can be reconstructed across computers, servers, user accounts, network devices, cloud platforms and security logs.

The role of IT is usually to make systems work again. The role of digital forensics is to determine what happened and preserve reliable evidence.

Both functions are essential, but they are not interchangeable.

The Most Valuable Evidence Is Often Temporary

Digital evidence is fragile.

Security logs may only be retained for a limited period. Cloud audit records may be overwritten. Endpoint data can change every time a computer is restarted or used. Temporary files, memory contents, active network connections and attacker processes may disappear when a system is shut down.

Restoring a server from backup may overwrite evidence showing how the attacker entered the system or what actions were performed.

Reformatting an infected computer may remove malware, but it may also destroy evidence of stolen credentials, lateral movement and data access.

Even well-intentioned troubleshooting can alter timestamps, create new log entries or change the condition of the affected system.

This does not mean that a company should avoid containment or recovery. It means those actions should be coordinated with evidence preservation.

The correct balance must be planned before the incident occurs.

The Delay in Appointing a Forensic Company

Many organisations do not have a digital forensic provider included in their incident response plan.

When an incident occurs, the company initially relies on its internal IT team or managed service provider. Several hours or days may pass before management accepts that external forensic expertise is required.

The organisation must then:

1. Identify suitable forensic companies.
2. Explain the incident to each provider.
3. Request and compare quotations.
4. Review confidentiality and contractual terms.
5. Obtain management or insurer approval.
6. Arrange system access and evidence collection.

During this process, the IT team may already be restoring servers, rebuilding computers, rotating accounts and reconnecting systems.

By the time the forensic investigators are formally appointed, the original environment may no longer exist.

The investigators are then asked to explain an incident using incomplete evidence. In some cases, they may be able to reconstruct part of the attack. In others, important questions may remain unanswered permanently.

This can leave management unable to confirm whether data was stolen, whether the attacker has been fully removed or whether regulatory reporting obligations have been triggered.

The Business Consequences of Poor Forensic Readiness

The loss of evidence is not only a technical problem. It creates business, legal and financial risk.

Without a reliable investigation, the company may struggle to:

- Make accurate regulatory notifications.
- Inform affected customers and business partners.
- Demonstrate compliance with data protection obligations.
- Support a cyber insurance claim.
- Defend itself in litigation.
- Determine whether ransom payment discussions are based on truthful attacker claims.
- Identify the original security weakness.
- Prevent the same attack from happening again.

Management may also be forced to make important decisions based on assumptions rather than evidence.

For example, the company may believe that an attack was contained because the encrypted systems were rebuilt. However, the attacker may still have access through a compromised account, remote access tool or cloud service.