RAPID RESPONSE

Richard Ford *examines the first 24 hours after a ransomware attack and asks: "What should you do?"*

A ransomware attack is a nightmare scenario for any organisation. It's disruptive costly, and often deeply damaging to your reputation. How you respond in the first 24 hours can make all the difference between containment and catastrophe. In those critical moments, fast and informed action is essential. Not just to mitigate harm, but to enable recovery and identify root causes. Whether you're facing a live breach or want to prepare your response strategy in advance, here's what needs to happen in the vital first 24 hours.

STEP 1: CONFIRM AND ISOLATE

The moment ransomware is suspected, the priority is to confirm what's happened. Ransomware doesn't always announce itself with a dramatic pop-up screen. It may begin quietly, encrypting files and spreading laterally across your network. Early signs might include inaccessible files, failed logins or unusual outbound traffic.

Once confirmed, isolate affected systems from the network immediately. Time is of the essence – ransomware often seeks to maximise damage by spreading across shared drives and cloud platforms. Disconnecting devices, disabling Wi-Fi and VPNs, and blocking access at the firewall level are essential to prevent further infection.

Having a cyber security team on standby allows for experts to provide step-by-step guidance in real time, helping you make the right moves to contain the threat without destroying forensic evidence. Having a calm, expert-led approach ensures you stay focused and strategic.

STEP 2: NOTIFY AND ASSEMBLE

Ransomware response is not just an IT issue, it's a business-wide challenge. Once containment is underway, inform key internal stakeholders, including executive leadership, legal, compliance and communications teams. Appoint a central response lead, ideally from your crisis management team, who can coordinate efforts and make key decisions quickly. If you've already established an incident response plan, now is the time to activate it.

STEP 3: SECURE AND AVOID ENGAGING

It may be tempting to click the ransom note or initiate contact with attackers to understand their demands. This is strongly advised against. Not only does it carry legal and ethical risks, but it may compromise your recovery options or make you more vulnerable to secondary attacks.

Instead, secure all backups and logs. Identify when the attack began, which systems are affected and what data may be at risk. This information will be crucial for both remediation and regulatory reporting. Having an expert partner will improve this process, by providing rapid forensic support to help assess the impact by identifying indicators of compromise (IOCs), tracing the attack vector and determining the attacker's dwell time. This information can also help you understand if data exfiltration occurred – an increasingly common element of modern ransomware.

STEP 4: REPORT & LEGAL OBLIGATIONS

Depending on your industry and location, you may have regulatory or legal requirements to report a ransomware incident. This could include notifying the Information Commissioner's Office (ICO), your industry regulator or affected third parties. It's important not to delay these conversations. Having clear documentation and technical insights to back up your reporting will help this process run smoothly.

STEP 5: RECOVER

Once the ransomware is contained and systems are stabilised, it's time to begin recovery. This involves more than just restoring files from backup. You must ensure the attacker's access is removed, vulnerabilities are patched and your environment is safe to bring back online. This is where a trusted partner makes all the difference. Incident response specialists will work alongside IT and cyber teams to validate clean systems, conduct a secure restoration, and put new protections in place. Your business shouldn't just bounce back, it should come back stronger.

Cyber security firms offer different ways to ensure organisations are ready to face ransomware. This includes emergency incident response, where teams can rapidly deploy to help take control, contain the threat and recover operations. Whether remote or on-site. Another option is to hold an incident response retainer, this is designed for preparedness. Retainer services give you guaranteed access to expert responders when you need them most. With predefined SLAs, threat intelligence and environment familiarity, these tools can help businesses respond faster and more effectively.

The first 24 hours of a ransomware attack are often chaotic, but don't have to be. With the right preparation and expert support, you can act swiftly, reduce damage and return to normal operations with confidence. When minutes matter, experience is your strongest defence ●

Ransomware doesn't always announce itself with a dramatic pop-up screen

Richard Ford is Chief Technology Officer at Integrity360.

Picture credit: AdobeStock