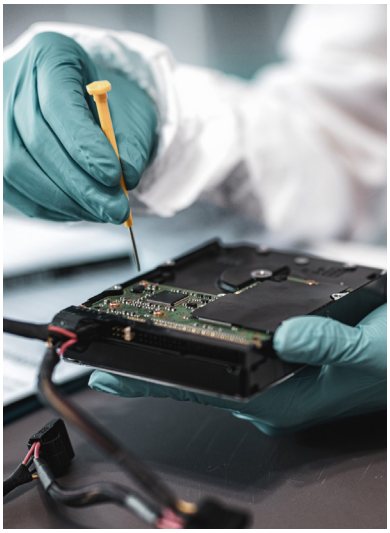
Case Study: Cost-Controlled Incident Response Contained Risk & Enabled Decisive Action



When potential insider risk intersects with encrypted activity and limited system visibility, organizations must act quickly – without overreacting or overspending. In this matter, a targeted incident response and forensic preservation engagement enabled leadership to understand the scope of risk, preserve defensible evidence for counsel, and take decisive action, all while avoiding unnecessary disruption or external exposure.

The Challenge

Security monitoring alerted the organization to unusually large volumes of encrypted data transfers originating from a company device assigned to a senior IT administrator. The activity occurred over a short time window and leveraged encryption, privacy tooling, and anonymized networks, significantly limiting traditional network-level visibility.

Security monitoring alerted the organization to **unusually large volumes of encrypted data transfers** originating from a company **device assigned to a senior IT administrator.**

Leadership faced multiple competing priorities:

- Preserve potentially critical evidence in a legally defensible manner
- Determine whether company systems or data were compromised
- Prevent further risk or spillage
- Brief the CEO with clear, factual findings – quickly
- Maintain discretion and control costs

Compounding the challenge, the sensitivity of the matter required careful handling to protect the organization while ensuring that any findings could withstand legal scrutiny.

The Strategy

A disciplined, decision-gated forensic approach was deployed to balance speed, rigor, and cost control. First, potentially relevant endpoints and removable media were secured immediately to prevent alteration, with full chain-of-custody documentation established from the outset. Devices were forensically imaged using industry-standard methods, and data integrity was verified through cryptographic hash validation.

The investigation proceeded along two coordinated tracks: a high-level enterprise cyber audit to assess systemic risk, and a focused forensic deep dive across multiple endpoints and electronically stored information (ESI) sources tied to the custodian. The scope of analysis was leadership decisions, or cost – ensuring that findings were actionable, defensible, and proportional to the actual risk identified.

Case Study: Cost-Controlled Incident Response Contained Risk & Enabled Decisive Action

Don't miss out on more free content from Team Avalon!

Join the Avalon mailing list to receive useful case studies, industry insights, handy tips, and more delivered straight to your inbox.

Sign up to receive exclusive content!

The Results

The investigation quickly surfaced facts that allowed leadership to protect the enterprise and act with confidence. Forensic analysis confirmed that:

- Encrypted outbound activity was linked to a commercial VPN and anonymized infrastructure, explaining gaps in network-level visibility
- Privacy and evasion tooling were used to route activity through anonymized networks and virtual machines
- The workstation was removed from normal corporate management, including abnormal administrative configurations and the presence of a hidden user profile
- Removable media contained a complete virtual system image, enabling work outside standard enterprise controls
- Evidence of trace deletion and system modification was identified, consistent with anti-forensic behavior

In parallel, a high-consequence discovery on a secondary device revealed material with potential criminal exposure. That evidence was preserved with strict controls and briefed privately to the CEO and counsel, enabling appropriate action while maintaining discretion.

Armed with defensible facts – not assumptions – leadership terminated the individual, implemented targeted containment and protective measures, and avoided external spillage or reputational impact. The entire engagement was completed in approximately 40 hours, with total cost under $25,000.

Deliverables included court-defensible chain-of-custody records, hash manifests, an executive-ready summary, a clear timeline of key indicators, and practical recommendations to reduce future risk.

QUESTIONS?

For more information on any of our services, please contact:

Rebecca Rudell, Marketing Manager
rebecca.rudell@teamavalon.com