

Global Healthcare Corporation Saves Millions of Dollars in Security Breach Incident

The average corporation experiences two data security breaches per year (*Third Annual ESI Trends Report – 2009*).

The Situation

A Fortune 100 healthcare organization engaged Kroll Ontrack when it had reason to be concerned that more than two million patient medical records were compromised during a data security breach. Kroll Ontrack quickly responded with a multidisciplinary team of legal and technical consultants whose strategic and tactical approach involved:

- » Extensive project management expertise to encourage savings and ensure a timely, seamless process from beginning to end
- » Implementing the industry's best practices and technology to determine exactly what happened
- » Building an organized approach to address and manage the aftermath of the security breach, ensuring regulatory compliance and proper notifications

The Solution

Based on its collective experience in getting to the bottom of data compromise incidents, the Kroll Ontrack consulting team took responsibility for overseeing all facets of the project, including:

- » Coordinating on-site data collection from 107 compromised hard drives and 17 servers in 32 multijurisdictional locations
- » Working with the client teams to respond to regulatory agencies
- » Analyzing varying information, including system logs and relevant data files, to evaluate the evidence and begin a series of field tests to construct the facts leading up to the incident

Ultimately, Kroll Ontrack consultants determined there was clear evidence that only a small fraction of medical records were compromised. However, it was also concluded that thousands of patient records had been placed at risk and that a notification program must be implemented. As such the fraud solutions team assisted the client in developing a communications response plan including a letter to the impacted individuals directing them to a call center with questions or concerns.

Early intervention narrowed the number of individuals impacted by the breach, reducing notification expenses by several million dollars. In addition, a news conference explaining the incident and remediation efforts took place within a week of the breach's discovery. As a result, the story went from a newsworthy headline to a mere back-page mention.

The Resolution

A nimble data security incident response strategy is critical to a successful outcome. In this case:

- » Impacted individuals were notified within two weeks of the breach's detection
- » Costs were substantially reduced through early detection and quick response
- » Negative public relations exposure was mitigated
- » IT security protocol was strengthened in preparation for future attacks, decreasing risk and costs related to future incident response