tracesecurity

# Case Study

Risk Assessment & Management

## The Company

A closely held healthcare organization based in the Midwest consists of over 15 medium-sized hospitals and clinics spread across five states. Most of the company's growth has been through acquisitions over a period of several years. The organization's IT infrastructure now serves over 800 full-time medical employees, certified physicians, and medical service contractors and vendors.

## Situation Overview

Before its rapid growth via acquisition, the company had no formal IT security and compliance program in place and was relying on a patchwork of spreadsheets and manual processes, which was managed differently across individual hospitals and clinics. Thus, there was no standard or any central point of authority or accountability for detecting and mitigating risks to sensitive data and the IT infrastructure. An internal review concluded that the organization's poor risk management posed a number of major problems, including:

- The management of over 450,000 patient records
- Ongoing dependence on unreliable and incomplete manual processes
- Poor oversight for more than 250 part-time, transitional, and outside users of the company's patient management system and EHR database
- A lack of formal reporting and cross-communication procedures: key departmental stakeholders, as well as C-level executives, were not receiving risk and compliance information in a timely fashion or in an actionable form.
- The danger of non-compliance with HIPAA regulations
- The need to improve and maintain the organization's overall reputation, as well as specific satisfaction ratings from patients, physicians, and staff

In the wake of these findings, the IT department was tasked to develop a comprehensive and unified risk assessment and management capability.

The universal message and takeaway from the summit was: Don't wait to get started, don't box yourself into a poor situation that doesn't fit, and don't overspend. The CEO and IT team walked away comfortable with this approach, and agreed that they needed a solution that was fast, flexible, and affordable.

## Solution Requirements

The organization faced both budget constraints and an ever-evolving risk and compliance landscape. Thus, managers representing IT operations, IT risk and security, compliance, and audit, determined that the proposed solution should include several key requirements, including:

- Ease of deployment and use (no extensive training or new specialized personnel required)
- Low installed cost
- Low total cost of ownership
- Should automatically update to recognize new risks as they develop in the market
- Should offer interoperability with other IT GRC functions, including audit management, training, change management, etc.
- Would allow the company to be prepared for a pending OCR and HHS audit within the next 60 days

tracesecurity

## Solution Options

The company organized a solution review team consisting of the CIO, Compliance Officer, Audit Manager, and VP of IT Security. In reviewing solutions from multiple vendors, the team determined that on-premise solutions were too expensive, would place a heavy burden on IT, and would take many months to implement. The administration costs and scaling challenges were of a particular concern.

They further decided that most of the available solutions, including managed solutions, required a long deployment cycle – some requiring six months or longer. Several vendors also required extensive contracts and high fees for solution updates and professional services.

The evaluation process ultimately yielded a consensus that the Risk Assessment and Risk Management functions of the cloud-based TraceCSO IT GRC platform met all of the company's most critical requirements.

## TraceCSO Solution – Advantages & Results

The team favored TraceCSO's Risk Management capabilities, first because of simple economics. TraceCSO's total cost of ownership was less half that of the nearest competitor, required no capital investment, and, because it is cloud-based, offered a much lower operational cost over the long term. TraceCSO didn't require extensive deployment costs typically associated with consultants or custom development. Besides the cost, the company's deciding factors had much more to do with performance and other strategic issues, including:

- Speed of Deployment – TraceCSO could be in place on-demand and fully deployed in their organization in just a few weeks, rather than months or years.
- Automated Functionality – TraceCSO made both Risk Assessment and Risk Management highly automated, eliminating the need for special training and averting the likelihood of errors.
- Depth – the Risk Assessment capability automatically identifies 37 threat categories and 85 discrete security controls, delivering a quick time to value for identifying risk and mitigation methods.
- Flexibility and Scalability – Because TraceCSO is cloud-based, the solution is automatically and transparently updated and can be easily expanded to scale as the organization grows.
- Interoperability – The solution integrates easily with other security applications and industry-standard tools such as vulnerability scanners.
- End-to-End Functionality – the TraceCSO platform offers several other functions that can be easily activated using the same data as the Risk function. These other functions will allow the organization to manages its vulnerabilities, internal audits, compliance reporting, vendor due diligence, and policies. As the organization's information security program grows, TraceCSO delivers seamless integration, a common user interface, and eliminates redundancy.

As a result of these new Risk Management capabilities, policies developed to manage risks are now uniform across all units of the company. The old manual processes have been eliminated, saving an estimated 68 hours per month in administrative time.

## Looking Ahead

With Risk Assessment and Management functionality in place, the company anticipates leveraging TraceCSO's vulnerability, audit, policy, and compliance management functions to further integrate and automates its IT GRC capabilities within a year.