Picking up the pieces after a data breach

Overview

No company likes being the victim of a data breach, however most companies will suffer a data breach at some point in their existence. One of the most common questions asked by those affected, state Attorneys General, and regulators is, "How will you ensure that this never happens again?" It is the response to this question that ultimately decides the reputational fate of the organization.

This is a case study where Special Counsel was engaged to assist a regional hospital in recovering from the aftermath of a ransomware attack that took place in the Fall of 2018. The team of cybersecurity professionals developed a methodology for evaluating the current state of the organization, making recommendations for improvements, and assisting the hospital with preparing for a visit from the U.S. Department of Health and Human Services (HHS).

The Background

Recently, Special Counsel had a case in which the cybersecurity team was tasked with developing and conducting an IT risk assessment that would measure the organization against compliance with the Health Insurance Portability and Accountability Act (HIPAA). The hospital had never been through the process before, which required the team to educate the client at the same time as they were asked to evaluate the current state of an organization that was notifying patients and employees of a data breach. To say that the mood at the hospital was tense, would be an understatement. However, by leveraging the values and ideals of Special Counsel, the team was able to complete the task within 30 days, under budget, and to the satisfaction of the client.

EQ

EQ is the legal consulting division of Special Counsel—the leading full-service provider of legal solutions. To learn more, contact your local EQ location today. specialcounsel.com

The Problem

A regional hospital in Texas was the victim of a ransomware attack in late 2018. The hospital realized that it needed help to identify its gaps and vulnerabilities. The challenge was to complete the task within 1 month and do it in the most efficient and cost-effective manner. Further, the organization had never been the victim of a cyber-attack, nor had they conducted a vulnerability and gap analysis. The hospital did not feel that they had the tools or knowledge to properly assess their current state, and how to remedy their gaps to comply with HIPAA and basic cybersecurity standards.

The Solution

Our team used its experience with HIPAA and the National Institute of Standards and Technology (NIST) Cybersecurity Framework, to develop a methodology for and scorecard for assessing the current state of the organization's information technology and information security environments. Our team then compiled a list of policies and procedures to review, and a list of key individuals to interview. The interview list included legal, human resources, information technology, and hospital operations staff members. The responses from the interviews and the results of the document review were then rated on a 1

(not being done) to 4 (excellent) point scale. A list of recommendations mapped to the Center for Internet Security's Critical Security Controls was provided to allow for actionable remediation steps.

The Costs

According to a 2018 Poneman Institute Report, the average total cost of a data breach is $3.86 million. Of that total cost, $1.76 million is spent on post data breach response activities include help desk activities, inbound communications, special investigative activities, remediation, legal expenditures, product discounts, identity protection services and regulatory interventions. A HIPAA violation has costs of $100 to $500,000 per record.

With these statistics in mind, the average NIST/HIPAA risk assessment for a single site company with under 500 employees will cost between $30,000 and $50,000. The implementation phase that follows the risk assessment has a variable range of costs based on the people, process, and technology needed to improve the infrastructure. In the present case, the implementation of improvements that need to be accomplished in the 30 to 60-day time frame was estimated to $100,000. In total, the process will cost roughly $150,000, well under the $3.86 million average breach cost.

When you consider the divergence in cost between the $3.86 million in average breach cost, the range of fines for HIPAA violations, and the $200,000 cost of improvements, the cost of being proactive far outweighs the cost of doing nothing and simply responding to a breach when it occurs.