EDWARDS
PERFORMANCE SOLUTIONS

CASE STUDY: ENHANCING CYBERSECURITY COMPANY WIDE BY IMPROVING STANDARD ASSESSMENTS AND DEVELOPING A PLAN OF ACTION WITH RELEVANT MILESTONES

SITUATION

When the Chief Information Security Officer (CISO) first joined a large US hospital, he reviewed the validity of the Health Insurance Portability and Accountability Act (HIPAA) compliance assessment performed by the auditing firm. There were no significant issues with the HIPAA assessment, but the CISO sought a new, more in-depth perspective that might identify the hospital's true high-level risks and related mitigation steps.

The CISO wanted an assessment that more closely followed NIST 800-53 and the NIST Cybersecurity Framework. Doing so would allow the hospital to be able to identify ways to bolster cybersecurity efforts in a way that HIPAA alone does not. Furthermore, it would lead to the hospital obtaining additional funding to grow and mature its security program.

In searching for assistance with revamping and implementing the assessment, the CISO discovered Edwards Performance Solutions.

> "Moving to the next level with plans of action and milestones is exactly what any security group really wants to see—that gives them responsibility to help move a program forward."
>
> **DANA PICKETT**
> Principal of Cybersecurity / Chief Information Security Officer
> Edwards Performance Solutions

SOLUTION

For the first three years of its partnership with the hospital, Edwards performed a HIPAA-meaningful use assessment. Edwards then mapped the assessment to both the NIST 800-53 and NIST Cybersecurity Framework. The resulting reports have led to the mitigation of risk from third parties.

"The hospital was questioned by an outside audit firm about the validity of how it's handling certain things, and the hospital was able to produce our report and be able to take that risk off the table," said Dana Pickett, the Principal of Cybersecurity and Chief Information Security Officer at Edwards.

SOLUTION | CONTINUED

The project scope expanded in the fourth year of the partnership when the hospital asked Edwards to establish a plan of actions and milestones (POA&Ms) based on the findings of the previous three years. This involved the following two-phase approach:

PHASE 1: EXAMINE THE PREVIOUS YEAR'S FINDINGS AT A GRANULAR LEVEL TO DETERMINE AND EXPLAIN ANY DIFFERENCES

PHASE 2: ASSIST THE HOSPITAL'S TECHNICAL OPERATIONS CENTER AND SYSTEMS OWNERS WITH DEVELOPING POA&MS

Currently, Edwards works with the hospital to help define the actual POA&Ms and provide guidance through the processes and tools needed to help move the hospital's overall cybersecurity program forward.

"This is what made this year very unique and very exciting for Edwards," said Dana. "What the POA&M engagement does is give us the ability to help the hospital identify resources and accomplish the actual elements of the plan, as well as put in the milestones to meet those tasks with scheduled completion dates. That's what the hospital has been looking forward to for three years now."

RESULTS

STRENGTHENED THE HOSPITAL'S CYBERSECURITY POSTURE
by going above and beyond standard mandatory HIPAA compliance

IDENTIFIED AND MITIGATED POTENTIAL HIGH-LEVEL RISKS
from third parties via reports

PROVIDED VALUABLE INFORMATION about every system and control at a granular level