*TREXIN CASE STUDY*

# UNDERSTANDING CYBERSECURITY'S RISK TO GROWTH

*Trexin helped a specialty Healthcare Payer conduct an independent cybersecurity assessment.*

## BUSINESS DRIVER

A small specialty Healthcare insurance company established aggressive growth goals to reach $1B in revenue. Given the relative importance of protected health information, the organization practiced security awareness but wanted a better understanding of organizational capabilities and current trouble areas that could impede the achievement of their growth goals. As part of a broader technical assessment, our Client asked us to conduct a focused Cybersecurity and Risk Assessment.

## APPROACH

Trexin's approach to cybersecurity is to follow the data to ensure effective and reasonable diligence to mitigate the ever-expanding threat landscape. Our first step was to conduct an independent assessment of existing cybersecurity capabilities with respect to people, process and technology within the organization. Working closely with technology leaders, subject matter experts, business units and cybersecurity personnel, we conducted interviews, covert breach testing and analyzed a specific set of documentation and process guides. The data we collected was measured against industry best practices including the National Institute of Standards and Technology (NIST) Framework and the Center for Internet Security's Critical Security Controls for Effective Cyber Defense (CIS CSC).

Upon developing a current-state Cybersecurity and Risk focused scorecard, Trexin presented the results in a familiar format leveraging the Capability Maturity Model Integration (CMMI) structure and reviewed that with the Client's project Steering Committee for alignment.

The final step in our approach involved the creation of a prioritized list of recommendations aimed at most efficiently and effectively addressing the capability uplifts needed to support the complex growth goals of the business. Some elements of this roadmap included staffing changes, metrics/monitoring enhancements, use of a CMDB, and Identity and Access Management (IAM) technique improvements.

### Focused Cybersecurity and Risk Assessment Leads to Growth Goals

Our Client, a specialty healthcare insurance company, enlisted Trexin to assess their Cybersecurity risk and current capabilities as it relates to their future growth.

### Follow the Data

To ensure the mitigation of threats to our Client, Trexin conducted a stepped approach to the assessment.

**STEP 1**

**Independent Assessment**
- Interviews
- Covert breach testing
- Analyzed processes

**STEP 2**

**Current State Scorecard**
- Results in CMMI format
- Shared results with Steering Committee

**STEP 3**

**Prioritized Recommendations**
- Staffing changes
- Metric enhancements
- IAM technique improvements

Trexin concluded that our Client's current capabilities could not accommodate future growth. An Enterprise level Risk Management committee was established and additional resources hired in order to help fortify itself against future issues.

## RESULTS

With Trexin's experience and expertise administering independent assessments, the Cybersecurity and Risk Management assessment successfully demonstrated how our Client could not accommodate future growth with their current capabilities. There was a mutual understanding that the current operating model required explicit, incremental adjustments to fortify itself against future issues. As a result, an Enterprise level Risk Management committee was established to begin the process of identifying risks to the business and establishing consensus on what responses to take. Additional infrastructure resources were also hired, and a third-party vendor analysis was initiated to identify partners to assist with a rapid-results minded capability build and knowledge transfer services.

## CONTACT US

**Healthcare Practice**
hc@trexin.com
www.trexin.com