Construction Services Firm Case Study

Data Protection/Privacy Controls Assessment of Key Application

Client Overview

Key Issues:

- Construction firm planned for migration of an on-premise, heavily-customized COTS application ('Key App") to a SaaS solution from the same vendor.
- Client conducts business with clients from heavily regulated industries, which led the CFO to sponsor a Data Protection/Privacy Controls Assessment of the application environment under migration.
- Core scope and deliverables of Assessment for Key Application
  - DBSA (tool for Oracle databases) data security controls and risks review
  - Sensitive data classification of one database ("*Critical Application*")
  - Data protection maturity mapping
  - NIST control framework review
  - Privacy protection controls for databases
  - Provide findings and roadmap to mature "*client's*" data security controls, and to mitigate risk of a data breach

How Our Consultants Helped

Summary of Findings (data collection, tools, and interviews conducted over three days):

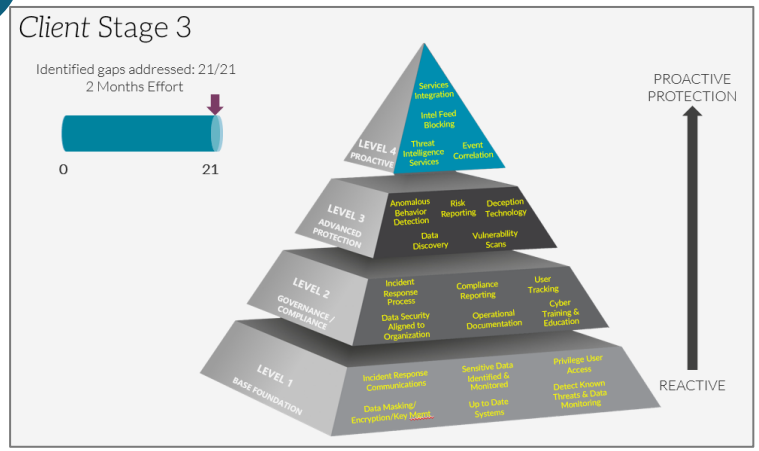
- 25 DBSA, "*Critical Application*" Data Classification findings across following categories:
  - Patching
  - Encryption
  - Test Data Management
  - Auditing
  - User Management
  - Configuration
- 8 NIST findings, 6 Privacy Findings, 14 Roadmap Recommendations
- Security Data: compromising usernames and passwords
- Financial Data: compromising account numbers, amounts, and salary information
- Personally Identifiable Information (PII): compromising national id numbers, names, addresses, personal dates, email and phone numbers
- Health Information (HIPAA): compromising patient and medication names

Results

Recommendations:

- Clear Roadmap for client to mitigate risk of data compromise in Key App over three stages (over 12 months) for 21 specific gaps, including time/budgetary estimates to remediate
- Manageable projects with clear outcomes for "*client*"
- Move data security from a reactive to a predictive security posture (see chart below)
- Roadmap recommendations aligned with NIST, CCPA & GDPR findings, and Data Protection Maturity Model

Data Protection Posture -- future state after Stage 3:



CrossGEN