Case Study

Security Assessment Services for Enterprise Client

Client:

Enterprise Business

The client is a Cincinnati-based company that maintains several lines of business in a variety of industries and under several regulatory bodies. The client's business lines include entertainment, logistics, retail, hospitality, marketing, and finance.

Challenges	CBTS Solutions	Results
• The client needs a formal security program that governs all of their businesses • The program must provide a baseline for each business line to follow, including policies, procedures, and controls • The program must provide metrics for leadership to measure each business line on its security maturity and growth over time	• CBTS assessment of the client's operational processes, documented and approved policies, and existing security controls and defenses • CBTS measurement and development of custom findings reports for each business line • CBTS delivery of a master summary report that provides guidance for the client's overarching program	• The client has security strategy to advance their maturity, increase risk management capabilities, reduce the attack surface for each business line, and improve overall corporate security posture • The client has confidence that they will continue to effectively protect their data and respond to threats as their computing environment grows and changes in the coming years

Security, covered.

Business Challenges

The client serves many business and consumer customers, and is expected to protect customer PII, financial information, and other sensitive data. Each client line of business is diverse – with a separate computing environment as well as some common assets and applications shared by many or all of the business lines.

Each business line also possesses differing levels of security maturity at the outset of this project. Some business lines are extremely capable with battle-tested processes and controls; others have an immature (or completely absent) formal security program.

The client requires a security strategy and roadmap to grow their security capabilities. The client's goal is to implement a formal security program that governs all of their businesses. The program needs to provide a baseline for each business line to follow, including policies, procedures, and controls. The program also must provide metrics for leadership to measure each business line on its security maturity and growth over time.

Leadership designates risk priorities, and is concerned about loss of financial and personal information, and public confidence due to a breach. Risk mitigation is ultimately the responsibility of the security program, as well as IT and security staff in each business line. The client needs to ensure their security program is capable of meeting these requirements.

Key questions include:

- What policies need to be in place to govern the behavior of all users of the network?
- What processes make up the operational rhythm of the security team?
- What technical controls and defenses provide protection and visibility?
- What metrics should be used to measure the effectiveness of the program?

CBTS Solutions

CBTS and the client have worked together on several IT projects, including deployment of network and server technologies.

The client engaged the CBTS Security Services team of consultants to help understand and improve their security posture.

CBTS worked with the client to plan a wide-ranging security assessment. Using the industry-leading Cyber Security Framework developed by the National Institute of Standards and Technology (NIST), CBTS evaluated the program in place at each of the client's business units.

The NIST Cyber Security Framework (CSF), developed and released by NIST in 2014, provides guidance to private-sector organizations on building a security program that can prevent, detect, and respond to security incidents. It describes five domains of operational responsibility for the security program and tiers to classify their capability – from Tier 1 (Partial) to Tier 4 (Adaptive).

CBTS' evaluation, conducted over the course of 90 days, included expansive assessments of operational processes, documented and approved policies, and existing security controls and defenses. CBTS consultants interviewed the client's IT and security staff, as well as company leadership, to understand risk and threat priorities as well as company culture and existing areas of responsibility. Each business line was measured and assigned a Tier. Following completion of the individual assessments, an overall Tier was assigned to the client.

CBTS Solutions (continued)

CBTS consultants developed custom findings reports for each business line. These included:

- Executive summaries that describe gaps and recommendations at a high level.
- A CSF Tier and goals for future growth.
- A roadmap describing the recommended initiatives to pursue in the coming 1-3 years to progress in maturity.
- Detailed descriptions of each discovered issue and recommendation, prioritized based on the importance and difficulty of implementation.

Finally, a master summary report that aggregated each of the issues observed at each business line, as well as those observed at an overall leadership level, provided guidance for the client's overarching program. The report addressed questions about the overall Tier of the client, expectation of growth in the coming years, and reasonable goals for Tier improvement in each business line, along with the people, processes, and technologies necessary for this growth.

Standards Used

- NIST Cyber Security Framework v1.0
- NIST Special Publication 800-53r4
- Center for Internet Security's Top 20 Critical Security Controls v6.1

CBTS Resources

CBTS deployed a team of experts to design and perform the engagements for the client. The team includes:

- An Account Manager
- A Senior Security Consultant
- A Security Engineer
- A Service Delivery Manager

Results

The client now has a security strategy to advance their maturity, increase their risk management capabilities, reduce the attack surface for each business line, and improve their overall corporate security posture. As the client's computing environment grows and changes in the coming years, including a planned migration of critical assets and applications to the cloud and the diversifying of internal assets to address mobility requirements, the client has confidence that they will continue to effectively protect their data and respond to threats.