TXY SAI

INTELLIGENT ECOSYSTEMS FOR BUSINESS & IT

Cut Yearly Cost Achieve cybersecurity **sustainability** by leveraging business practices
Increase Executive Participation CxO + board **engagement** accelerated involvement
Close Gaps at Your Weakest Link Develop an ecosystem to measure **third parties**
Leverage the Power of Simulations Proactively **align** GRC with PR best practices
Take Your Experts to the Next Level CISO **mentorship** program, business training
Leverage the Power of Operations Develop a program of **shared responsibilities**
Leverage the Power of Culture Over Strategy **Reduce** cost, time, and overall effort
Cut Time Utilize the powerful self-assessment Cyberator that **accelerates reporting** by 75%

We have designed and run Cybersecurity programs for multiple organizations, our largest one affecting 75,000 employees & 500+ departments

BLUE CYBER LABS

Let us help you shape and mold the critical elements of your organization, towards greater cybersecurity maturity.

Tools & Cybersecurity Expertise are no longer enough.

WE ARE SEASONED EXPERTS THAT BUILD SOLID AND LASTING ECOSYSTEMS BETWEEN BUSINESS & IT, for the purpose of creating a 'threat prepared' culture in all areas of your organization. This makes you more sustainable, creates intelligent redundancies, reduces drastically your cost, and minimizes your risk.

3 OPTIONS

OPTION 1: 30-60-90-day ecosystem proprietary methodologies applied (cyber spheres)
It includes all business and IT strategic direction and decisions for proper funding/effort/staffing
Within 2 weeks: 3 scenarios and 3 simulations for the most complex upcoming decision making

OPTION 2: 30-60-90-day sustainability and valuation methodologies and roadmaps created
It includes all business and IT governance, CISO mentorship program, and PR elements included
Within ½ day: maturity score obtained (including cyber and governance frameworks) + reports

OPTION 3: 30-60-90-day traditional technical assessment with risk analysis, scans and tests
It includes all NIST & other applicable framework controls assessment (depending on industry), gap analysis, detailed findings, recommendations, and roadmaps

TXYSAI – contact@y-sai.com - 8087215141

SAMPLE ENGAGEMENT

Duration

4 Weeks (on-site/off-site)
Team: 4 individuals (2 on-site)

Scope

Sustainable Cybersecurity within the organization's Ecosystem of People/Process/Technology

- Information Gathering
- Baseline Analysis
- Gap analysis
- Controls Identification
- Threat Identification
- Risk assessment
- Comprehensive Strategic Roadmap
- Executive Presentation
- Executive Summary
- Prioritization Action Plan for Mitigation & Remediation
- Industry Standards
- Comprehensive Policy templates
- Quantifiable maturity scores of your current Cybersecurity program
- Opportunity matrix
- PMP style reports with tasks that can be assigned to the team immediately
- A list of resources that will assist you in finding security products that implement the Critical Security Controls: Resources for setting up your security awareness programs; Gaining Support for Security Awareness Programs; Security Awareness Program Planning; Measuring Security Awareness Program Results
- Your common regulatory obligations based on your industry and region;
- List of questions a CISO is likely to face when presenting to top management;
- Steps to take after a data breach
- A Public Relations analysis for preparation in the event of a security breach
- A legal perspective on prioritization of remediation steps
- A decision-making process, which will prove crucial when having to decide where and how to invest resources in the cybersecurity defense landscape.