Problem: Today's complex cyber threats pose severe and costly risks to Government and commercial organizations, including data theft, infrastructure breaches, and supply chain infiltration. In an IoT world, the nature and severity of cyber threats have evolved, and so must organizational approaches to cybersecurity. Defending against modern cyber threats, however, is a daunting task for many commercial and Government agencies. A reliable cyber assurance evaluation requires specialized expertise and a commitment to full transparency across an organization's operations. Many organizations lack resources necessary to conduct a thorough, objective self-evaluation of their cybersecurity position. Equally critical, and lacking by many organizations, are the resources to implement controls, manage assets, and train personnel to sustain cybersecurity health.

Solution: STS uses an integrated, multi-level lens to approach today's cyber challenges, applying proven technical and people-focused solutions to securing the enterprise. Our approach to defending Government agencies and private organizations includes four tenets:

1) A multi-level, comprehensive view of the cyber ecosystem to include people, supply chains, and the network of interconnected assets (physical and digital)
2) The integration of offensive and defensive cyber tactics to assess and defend
3) An independent, third-party evaluation to enable objective and rigorous assessment
4) A sustainable cyber assurance plan to adapt to evolving threats Organizations operate within a vast range of dynamic interactions and information exchanges.

Sophisticated global supply chains and networks increase the complexity of, and risk to, an organization's cybersecurity. Therefore, successful cyber assurance requires a multi-level and comprehensive perspective, from the individual user and singular component to the enterprise network and complex system of systems. We evaluate vulnerabilities in an enterprise's inherently linked supply chain, cloud systems, and networks as well as people's interactions within its ecosystem. STS's cyber solutions manage supply chain risk, track hardware and software, secure personnel processes and work flows, and ensure the proper use of assets. Our engineering and materials development capabilities can provide secure, optimized hardware alternatives to supply sources. Additionally, we employ a multi-level approach to implement security controls for individuals, small to mid-size teams, and large divisions within an organization.

Securing the enterprise must also unite offensive cyber penetration testing to find the gaps with defensive cyber safeguards to close the gaps. To truly test and validate cyber defenses, an objective, third-party assessment must be operating outside the organization's influence. Rigorous penetration testing from the outside-in reveals gaps in an organization's cybersecurity, while also examining the effectiveness of its defense mechanisms. STS helps customers find vulnerabilities in their systems/devices and address the gaps.

Personnel training is critical to cybersecurity as the end-user is the biggest threat within information systems. Our programs teach end-users about phishing, ransomware, and other click bait attacks, which are the top threats to organizations. STS's complete end-to-end solution synchronizes personnel training, policy development, testing, asset management, and sustainability planning to enhance organization's cyber resilience. STS solves what are completely overwhelming cyber challenges to many clients, providing Government agencies and private industry a complete framework against modern threats.