SYNERCOMM

Standards-based Security Planning with OneSSP®

Stop letting cybersecurity manage you.

Manage your cybersecurity instead with data-driven objectives, trackable key results, and measurable outcomes

Businesses meet their customers where their customers are. Businesses and customers now broadly interact in on-line and virtual environments. On-line and virtual environments facilitate rapid innovations and improvements to customer experience and accelerate changes in customer expectations. Businesses must continuously respond to those expectations or risk ceding business to their competitors. IT organizations must continuously innovate and develop information technology to keep pace, which comes with continuously increasing cybersecurity risk exposure. If not organized and managed properly, that exposure will result in catastrophic business impact. OneSSP® helps remove the guesswork around organizing and managing a cybersecurity program. OneSSP® facilitates a data-driven set of initiatives that are standards-based and trackable with measurable, risk-prioritized outcomes.

Stop letting cybersecurity manage you…

Qualified cybersecurity human resources are in short supply while demand is high. Organizations want action and results. The combination of these two conditions commonly results in a disorganized and reactive cybersecurity posture with high turnover rates among cybersecurity resources. Because of this, many businesses focus on short-term, tactical security operations, and often seek quick fixes through outsourced cybersecurity operations and/or specific security solutions. This approach leads to a false sense of security and a blissful ignorance of the ever-growing risk the business faces. When a security event inevitably occurs these businesses often react with more short-sighted changes, hoping for but not realizing different results. Hope is not a strategy, and so this ineffective and inefficient cycle continues until the business improves its approach to cybersecurity or fails to recover from a catastrophic security event.

Manage your cybersecurity…

Leading security experts contribute and collaborate to develop and maintain cybersecurity frameworks. Cybersecurity frameworks define standards and best practices for managing the most common cybersecurity risks. Properly utilized, a cybersecurity framework can serve as the backbone for an organized, managed, tracked, and measured cybersecurity program; a program that facilitates continuous improvement in cybersecurity maturity and risk management. OneSSP® leverages frameworks appropriate for the unique circumstances of each customer for effective and efficient planning, execution, operation, and validation of a data-driven, risk-based cybersecurity program.

How it Works

- Understand business regulatory requirements and IT operating environment
- Discover IT business services and conduct a high-level business impact analysis for each
- Select appropriate framework(s) and goals
- Map IT business services to the framework
- Conduct a gap assessment and quantify current-state security maturity business service risk
- Document a budgetary (cost/quality/schedule) Plan of Action and Milestones (POAM)
- Instantiate and manage cybersecurity program, track progress (POAM) and outcomes (gap closure)
- Operate, validate and continuously improve

Organizations who benefit the most:

- Organizations struggling to develop / maintain good cybersecurity
- Organizations seeking validation of their cybersecurity program and posture
- Organizations with regulations or customers who require an organized cybersecurity program
- Ready to integrate cybersecurity risk management into broader enterprise risk management

Manage your cybersecurity lifecycle with OneSSP®

With OneSSP®, you benefit from having a team of experienced cybersecurity experts helping you build and manage an effective and efficient cybersecurity program. Effective because the program is standards-based, risk-informed, and data-driven. Efficient because program activities are prioritized according to business impact. SynerComm's OneSSP® execution, operation, and validation services scale up or down in accordance with customer needs. SynerComm can provide continuously active support of your cybersecurity program or can simply provide continuity of operations in times of employee transition. OneSSP® helps you escape the cycle of reactive cybersecurity and instead build an organized, standards-based cybersecurity program that can proactively adapt to an ever-more-dangerous cybersecurity threat landscape.

More Thoughts/Ideas:

Cybersecurity programs require a variety of different technical, operational, and security skillsets at the various stages of program development and execution. SynerComm has a diverse team experienced in Information Assurance, IT Solutions, Project Management, NOC/SOC, and Technology Sourcing.

Cybersecurity is fraught with black swans (those things we do not know that we do not know). Some apply while others do not for each customers' unique needs. SynerComm's OneSSP® team of experts provide relevant education that helps you understand and navigate through those unknowns.

Benefits:

As-needed flexible resourcing

(use SynerComm a little or a lot as your organization's particular needs require)

Continuity of operations

Having a highly capable and flexible third party intimately familiar with your environment can insure against the transition of key cybersecurity team members. SynerComm can step in temporarily to support duties and train replacements.

What-if analysis

With OneSSP® you can preview anticipated residual maturity and risk values assuming the successful execution of the prioritized POAM.

5-year budgetary planning

SynerComm translates the POAM automatically into a 5-year estimate of cost (implementation and ongoing operation) and effort (full-time equivalents for implementation and operation).

plan and execute a security program that protects for your business in the face of constantly evolving cybersecurity threats.

SYNERCOMM