U.S. Small Business Administration

Cybersecurity

Protect your business & understand compliance requirements

Register for critical FREE interactive web-based training:
https://synergysolutions.talentlms.com
Registration Required

You Will Learn:

Participants will learn critical cybersecurity concepts and approaches to protecting their resources and intellectual property, and mandatory federal directives and contracting requirements for prime and subcontractors.

- Courses assist 7(j) contractors understand DFARS 252.204-7012 (Jan 2019) and NIST 800-171 r1 compliance requirements. Participants also receive up-to-date news on the DoD Cybersecurity Maturity Model Certification (CMMC) program.

- Individual course enrollment instructions provided after participants set up their user ID, password and register their 7(j) eligibility information in the Learning Management System (LMS).

- It is encouraged for courses to be taken sequentially, but not required. Eligible 7(j) participants completing modules 1-10 will be provided 30 day access to a FREE Tool that they can immediately use to assess their company's cybersecurity risk and provide information on how to improve their security posture.

- A detailed summary of classes and training calendar are attached and available at https://synergysolutions.talentlms.com.

Who can participate? Small business owners who:

- *are* certified 8(a) participants
- *have* a HUBZone certified small business
- *have* an economically disadvantaged women-owned small business
- *have* a small business located in areas of high unemployment or low income
- *have* a small business owned by low income individuals

7(j) MANAGEMENT AND TECHNICAL ASSISTANCE PROGRAM TRAINING

Training Provided by:

SYNERGY solutions

For Help Desk contact:

john.anderson@ssi-synergy.com or
charles.givens@ssi-synergy.com or
call 865-471-8192 (8 am - 5 pm ET)

For more information about the 7(j) program, please contact your SBA District Office. You can find local office information at www.sba.gov/tools/local-assistance

SBA Cybersecurity Training Schedule – Nationwide

November 2020

*Training courses are individual stand-alone courses; however, Introduction to Cybersecurity courses/modules (Mods 1-10) are encouraged to be taken in sequential order for cybersecurity novices as definitions and concepts from previous modules may be referenced in later courses. It is the participant's responsibility to track what training courses they have registered for and to sign-in for the course at the designated date and time. All training offerings are posted using Eastern time zone. Classes may be cancelled and rescheduled if a minimum of 5 participants is not reached one day prior to the subject class offering. (*Note: The Cybersecurity Tool will be released to 7(j) participants after all 10 courses/modules are completed.)*

MON	TUES	WED	THURS	FRI
NOV 2	**3** 1 – 2 pm ET: MOD 5 2:30 – 3:30 pm ET: MOD 6	**4** 1 – 2 pm ET: MOD 1 2:30 – 3:30 pm ET: MOD 2	**5** 1 – 2 pm ET: MOD 7 2:30 – 3:30 pm ET: MOD 8	**6** 11:00 am-12:00 pm ET: MOD 3 12:30 - 1:30 pm ET: MOD 4
9	**10** 1 – 2 pm ET: MOD 9 2:30 – 3:30 pm ET: MOD 10 **Tool Open (30 days)*	**11** 1 – 2 pm ET: MOD 5 2:30 – 3:30 pm ET: MOD 6	**12** 1 – 2 pm ET: MOD 11 2:30 – 3:30 pm ET: MOD 12	**13** 11:00 am-12:00 pm ET: MOD 7 12:30 - 1:30 pm ET: MOD 8
16	**17** 1 – 2 pm ET: MOD 1 2:30 – 3:30 pm ET: MOD 2	**18** 1 – 2 pm ET: MOD 9 2:30 – 3:30 pm ET: MOD 10 **Tool Open (30 days)*	**19** 1 – 2 pm ET: MOD 3 2:30 – 3:30 pm ET: MOD 4	**20** 11:00 am-12:00 pm ET: MOD 13 12:30 - 1:30 pm ET: MOD 14
23	**24** 1 – 2 pm ET: MOD 15 2:30 – 3:30 pm ET: MOD 16	**25**	**26** Thanksgiving Holiday	**27**
30	**Dec 1** 1 – 2 pm ET: MOD 5 2:30 – 3:30 pm ET: MOD 6	**2** 1 – 2 pm ET: MOD 1 2:30 – 3:30 pm ET: MOD 2	**3** 1 – 2 pm ET: MOD 7 2:30 – 3:30 pm ET: MOD 8	**4** 11:00 am-12:00 pm ET: MOD 3 12:30 - 1:30 pm ET: MOD 4

U.S. Small Business Administration

Funded through a contract with the U.S. Small Business Administration. SBA's funding is not an endorsement of the contractor or any products, opinions, or services. All SBA programs are extended to the public on a non-discriminatory basis.

Training courses are individual stand-alone courses; however, Introductory Cybersecurity modules 1-10 are encouraged to be taken in sequential order for cybersecurity novices as definitions and concepts from previous modules may be referenced in later courses. It is the participant's responsibility to track what training courses they have registered for and to sign-in for the course at the designated date and time. All training offerings are posted using Eastern time zone. Summary notes handouts of each course will be distributed to participants in attendance. Each course is approximately 1 hour and includes time for direct interaction and Q&A with the instructor.

CYBERSECURITY – HOW TO PROTECT YOUR BUSINESS ASSETS AND CUSTOMERS
INTRODUCTORY CYBERSECURITY MODULES (1-10)

Module 1 - Why Cybersecurity?
In this module, we'll discuss what cybersecurity means for your company, employees, partners and customers. We'll consider what makes your company vulnerable, how data breaches occur and some steps you can take to protect your company and your data. Finally, we'll explore some of the laws and contracting requirements that specifically apply to companies doing business with the Federal Government or their prime contractors.

Module 2 - Cybersecurity Basics
This module is specifically focused on fundamental concepts of cybersecurity. We'll discuss the goals, objectives and essential objectives of cybersecurity programs and how successful programs are implemented. Finally, we'll consider some specific foundational activities like good password discipline, effective strategies for backing up data and elements of effective cybersecurity policies to help protect your business assets and reputation.

Module 3 - Endpoint Security
In this module, you'll learn about how endpoint devices such as laptops, desktops, tablet computers and mobile devices can offer cybercriminals a gateway into your company's networks and data. We'll discuss the various types of endpoint devices, what makes them vulnerable to exploit by cybercriminals and how to protect them from attack. We'll also discuss one of the basic concepts of cybersecurity – defense-in-depth.

Module 4 - Network Security
Securing your network is one of the basic tasks of providing cybersecurity for your company. In this module, we'll discuss what it takes to properly secure a business network, explore the various threats networks commonly face, and how the concept of defense-in-depth applies to protecting your network. Finally, we'll consider specific network protection tools, such as Intrusion Detection/Intrusion Prevention Systems (IDS/IPS), firewalls, Network Access Control programs and anti-virus/anti-malware systems.

Module 5 - Data Security
The bottom line of cybersecurity is providing protection for your company's data and that of your customers and partners. This module will discuss why protecting data should be at the heart of your cybersecurity program, the types of data you are responsible for and threats to that data. We'll introduce and discuss the concept of individual cyber hygiene and discuss a case study of one incident where data security broke down and the serious consequences that followed.

SBA

Funded through a contract with the U.S. Small Business Administration. SBA's funding is not an endorsement of the contractor or any products, opinions, or services. All SBA programs are extended to the public on a non-discriminatory basis.

INTRODUCTORY CYBERSECURITY MODULES (1-10) - CONTINUED

Module 6 - Security Frameworks and Standards

In this module, you will learn about cybersecurity standards and discuss several frameworks that are relevant to cybersecurity. We'll explore U.S. and international cybersecurity frameworks, including a detailed discussion of the National Institute of Standards and Technology (NIST) framework and cybersecurity standards specific to federal government contractors and to entities that process or store credit card data.

Module 7 - Laws and Regulatory Compliance

The Internet has often been equated to the lawlessness of the Wild West, but the reality is much different. While many types of behavior flourish on the Internet, nations and international bodies are slowly developing legal and regulatory frameworks to help bring order to the chaos. In this module, we'll discuss State, Federal and international laws and regulations you and your company will be expected to follow when you have a data breach or possess and process your customer's or employee's sensitive data. Finally, we'll explore the expectations various groups (e.g., the public, customers, media) will have of you if your company suffers a data breach.

Module 8 - Breaches, Security Crises and Incident Response

In this module, we'll conduct a detailed exploration of the targets, motivations and techniques of hackers, as well as various types of common attacks. We'll transition to discussing the incident response cycle and cyber investigations. We'll conclude with new developments in cybersecurity such as the rise of the use of cyber threat intelligence and how third-parties who handle or process your data may prove to be a previously unconsidered area of risk.

Module 9 - Prevention and Remediation

Preventing data breaches and incidents is a subject that is often a source of great discussion. In this module, we'll consider some basic truths about cybersecurity and data breaches, as well as some limitations of your cybersecurity efforts. We'll discuss how not to be a data breach victim, as well as outline some steps you can take to decrease or mitigate your company's risk of a data breach. Finally, we'll explore remediation steps you need to take should a breach occur to quickly recover and lessen the chances of reoccurrence.

Module 10 - Management Responsibilities and the Cyber Future

As the CEO or senior leader of your business, you have specific requirements when it comes to cybersecurity. This module will explore how executives must take responsibility for their company cybersecurity efforts and support and oversee these efforts. We'll discuss specific threats to small businesses, such as ransomware, phishing and theft of data and end with a review of the techniques cybercriminals to steal credit card data.

Cybersecurity Assessment Tool

Once a participant receives credit for passing Modules 1-10 cybersecurity training courses, they will be granted 30 day access to the Small Business Cybersecurity Assessment Tool 1.2, which is based on NIST 800-171, r1 and majority of the DoD CMMC criteria. The tool will help assess their business's cyber maturity and receive improvement recommendations to get to the next step for their business. Reports identify cyber vulnerabilities/risks and provide improvement recommendations. Tool database is secure, and no information is retained after the trial 30-day period from the user's initial protected access date to maintain information security protocols.

SBA

Funded through a contract with the U.S. Small Business Administration. SBA's funding is not an endorsement of the contractor or any products, opinions, or services. All SBA programs are extended to the public on a non-discriminatory basis.

INTERMEDIATE CYBERSECURITY MODULES (11-16)

Module 11 - Building a Cybersecurity Plan

This class will cover details on how to develop a cybersecurity plan for a small business, including online references, sample plans and various items of interest in security planning. Students will be expected to complete their own small business security plan based on the templates and information provided in the class. These plans will be reviewed by the instructors and returned with comments and suggestions. Reports from the *Cybersecurity Assessment Tool* (available after completing Modules 1-10) will assist businesses identify their cybersecurity maturity, risks and incident response readiness.

Module 12 – Evaluating Your Cybersecurity Program

How ready is your small business to deal with a serious cyber incident? Like many other aspects of a small business' daily life, the possibility of a serious cyber incident should be considered and planned for BEFORE it happens. This class will help participants think through how they need to respond during various phases of different types of cyber incidents. It will also discuss the elements of a good plan for responding to incidents and help participants prepare simple incident response plans for their own small businesses.

Module 13 – Cyber Incident Response

Responding effectively to cyber incidents, including notifications and root cause determinations, can be some of the most daunting experiences in the life of a small business. This class will discuss basic concepts in response, investigations, and determination of root cause in a suspected or actual cyber incident. Taught by experts experienced in leading businesses through cyber incidents, this class will also include hints and inside information on dealing with customers, employees, regulators and law enforcement during the stress and uncertainty that accompanies a serious cyber incident.

Module 14 – Federal Breach Notification Requirements

Federal government contractors who handle sensitive unclassified or personal data for the Federal government recently became responsible for reporting incidents involving potential or actual loss or compromise of that data. These requirements, along with requirements for cybersecurity planning by contractors, have been incorporated into the Defense Federal Acquisition Regulation (DFAR) and will most likely be made part of the overall Federal Acquisition Regulation (FAR) soon. This will require cybersecurity planning for almost all Federal contractors. This class will discuss the specific nuances of breach reporting for Federal contractors and give participants a glimpse at what changes to expect to Federal contracting procedures regarding cybersecurity.

Module 15 – Securing Cloud Services

This class will provide detailed discussion on how to maximize security when using cloud-based storage and services. Following a brief overview of cloud types and models, we will look at the main areas of concern when using the cloud, and steps you can take to address those concerns. Service contract terms and their negotiation will be covered.

Module 16 - Securing your Online Life

This class will discuss how to secure both a small business' online presence and the online life of the individual participant. Improving security settings for common social media applications, such as Facebook and Twitter will be covered, as well as discussion of tools to help make daily online life easier and more secure

SBA

Funded through a contract with the U.S. Small Business Administration. SBA's funding is not an endorsement of the contractor or any products, opinions, or services. All SBA programs are extended to the public on a non-discriminatory basis.