Small and Medium Business Cybersecurity & Defending Heavy Duty Vehicle Certification Bundle

BROCHURE

Lessons – Titles, Descriptions, and Objectives & Knowledge Gained

Lesson Title	Description	Course Objectives & Knowledge Gained
S1.1 Business Cybersecurity Threats and Risks	This lesson defines common cybersecurity terms and definitions, types of threats against small and medium businesses, and who is behind these threats. The module also explains common cybersecurity attacks such as malware, ransomware, business email compromise and how these attacks are usually carried out. Finally, it explains how cybersecurity threats impact small and medium businesses.	- Learn common cybersecurity terms and definitions - Understand the types of cybersecurity threats facing small and medium businesses - Understand who are behind the threats and what motivates them - Understand common attacks such as malware, ransomware, and business email compromise and how the attacks are carried out - Obtain a fundamental understanding of the existential threat these risks pose to the small and medium businesses
S1.2 Introduction to Cybersecurity Basics	This lesson covers the NIST cybersecurity framework as conceptual tool for understanding and protecting small and medium businesses. It explains how to identify what needs to be protected, how to identify risks and the basics required to protect a business. Additionally, the module explains, at a high level, how to detect and respond to cybersecurity events and recover. The module also includes additional external cybersecurity information links and resources. Lastly, a hands-on case study runs through a practical exercise on asset identification, risk identification and mitigation.	- Understand the components, phases and maturity levels of the NIST Cybersecurity Framework - How to identify technology and information assets, as well as critical business processes - How to identify, measure, and prioritize risks to your business - How to reduce and mitigate risks using technology and business processes - Understand the basics of the detecting, responding and recovering from an event using the NIST Framework - High level understanding of cybersecurity incident reporting requirements - Importance of an incident response plan in recovery phase - An introduction to the Center for Internet Security (CIS) controls which work well in conjunction with the NIST Framework

S1.3 Firewalls, Email Security and Endpoint Protection	This lesson covers the basic technical background and concepts for firewalls, email security and end point protection which are essential components in protecting any business. It also provides general guidance on how to select an appropriate vendor for each category, as well as some specific vendor recommendations.	- Understand the basic purpose of firewalls, email security, and endpoint protection and how they work - Criteria that should be used when looking for a vendor/supplier for firewalls, email security, and endpoint protection
S1.4 Computer Equipment Setup and Configuration	This lesson covers best practices for password management, recommendations on how to limit the use of administrator accounts, and provides an overview of how to configure Microsoft Windows and Apple Mac Book computers for improved security. Additionally, this module reviews useful check lists on where and how to identify dangerous vendor default passwords. It also provides references to public resources for more advanced and operating system specific configuration recommendations, as well as advanced tools to take the concept to the next level. The module also provides a brief high-level introduction to network security scanning tools.	- Understand default configurations and passwords need to be changed - Best practices for password management and limiting the use of powerful administrative accounts - A high-level understanding of the Windows Security Center, as well as essential information on how to configure Windows and Apple Mac Book computers for improved security - Checklists for finding default passwords, unused features, and software which should be disabled or uninstalled - Additional public resources for delving deeper into secure computer configurations and what tools are available to assist in larger environments - High level understanding of network security scanning tools and how they can be helpful
S1.5 Maintaining and Monitoring Your Environment	This lesson provides a practical approach on how to keep your systems and network devices updated with the latest updates and patches, as well as how to setup monitoring of your equipment and network environment.	- The attendee will understand why updates are necessary and how to update the most common computer types, as well as best practices for applying updates - Learn the importance of performance and event monitoring, and learn some key strategies on how to implement monitoring inside a small and medium business
S1.6 Building Resilient and Recoverable Environments	Lesson covers detailed strategies on how to design and build computer environments that are resilient and are able to recover from adverse events. This includes backup terminology, strategies and best practices. Also covered is the planning, policies, procedures, and documentation that supports a resilient and recoverable environment. A case study is included to walkthrough a sample SMB environment.	- Learn common backup terms, strategies, and best practices - Understand the basics of planning and artifacts, such as incident response plans, system documentation, and recovery procedures - How written company policy can be used to enforce the development and maintenance of key artifacts required for a resilient environment

S1.7 Managed Service Providers	Lesson provides an overview of managed service providers and the tradeoffs in using them. Module covers specific information and suggestions on how to find, evaluate, compare and select an MSP, as well as MSP contract reviews, understanding the onboarding process, and how to mitigate MSP vendor risk.	- Understand what an MSP is and what services they provide - The tradeoffs involved in using MSP as opposed to internal staff - How to find MSPs in your area with relevant industry experience - How to evaluate, compare and select an MSP - Pitfalls to watch for in MSP contracts - How to mitigate the risks that an MSP can pose to a business
S1.8 Defending Heavy Duty Vehicles *(as standalone lesson or within the series bundle)*	This lesson provides an overview on identifying and mitigating risks posed to small and medium businesses who operate heavy truck fleets.	- Understand the unique cybersecurity threats against trucking companies and heavy vehicles, such as BYO devices, USB drives, HD radio, Bluetooth, telematics/ELD devices, general RF attacks, maintenance system/tools and service providers - General concepts and strategies for risk mitigation - How to get help if your heavy vehicles experience a cyber attack