# *SBA Cybersecurity for Small Businesses*

## *1.1 Introduction*

Welcome to SBA's online training course: Cybersecurity for Small Businesses.

SBA's Office of Entrepreneurship Education provides this self-paced training exercise as introduction to securing information in a small business. You will find this course easy to follow and the subject matter indexed for quick reference and easy access. It will take about 30 minutes to complete the course. Additional time will be needed to review included resource materials and to complete the suggested next steps at the end of the course.

As audio is used throughout the training, please adjust your speakers accordingly. A transcript and keyboard shortcuts are available to further assist with user accessibility.

When you complete the course, you will have the option of receiving a completion confirmation from the SBA.

## *1.2 Course Objectives*

1. The course has six key objectives:
2. Define Cybersecurity.
3. Explain the importance of securing information through best cybersecurity practices.
4. Identify types of information that should be secured.
5. Identify types of cyber threats.
6. Define risk management.
7. List best practices for guarding against cyber threats.

## *1.3 Course Topics*

This course will address four areas, defining the importance of information security and what you can do to keep your information safe:

- What is cybersecurity?
- Why is cybersecurity so important?
- What are common cyber threats and crimes?
- How do I determine my level of risk?
- What can I do to protect my business?

Numerous additional resources are identified to assist you. Visit the resource icon in the course player or locate additional tools, templates, and mentors on SBA.gov once you finish the course.

Let's get started!

## *1.4 Background*

Cybersecurity is the comprehensive effort to protect computers, programs, networks, and data from attack, damage, or unauthorized access through technologies, processes, and best practices. Large businesses have been working to secure their information and systems, so small businesses are becoming more common targets because they have fewer resources than large companies have. Do you have information that needs to be secure? Consider:

- Personal information for employees
- Partner information
- Sensitive information for customers/clients
- Financial and sensitive business information

Information needs to be secured in your systems. This means the information that should be kept confidential should be available when needed, and should be kept as accurate as possible. Your website also needs to be secure in order to prevent putting current or potential customers at risk.

## *1.5 Aspects of Information Security*

There are several different aspects of information security, including confidentiality, integrity, and availability.

Some considerations for confidentiality include: only those who need access to information, and have been properly trained on cyber security, should have it, especially when the information is sensitive. Training people in cyber security prevents security breaches when those who are authorized accidentally disclose information. Your goal should be to ensure information is not disclosed to non-authorized people.

Considerations for integrity include making sure your information is not improperly modified or destroyed. If you maintain information integrity, no one will be able to claim your information is inaccurate.

Last is availability. Your information should always be available to you quickly and reliably.

## *1.6 Security Costs*

It is important to remember that there are costs for protecting information; there are also costs for *not* protecting information, which will be covered later in the risk topic.

The costs for not protecting information can be much higher than those associated with protecting it. These costs could be associated with notifying victims that their information has been released, which can be very costly, both in terms of perception and litigation. You can lose customers who have lost confidence in your business after a security breach. Depending upon the type of business you have, you may have to pay

fines for not maintaining information security compliance. You may also have to reconfigure or replace hardware and/or software.

## *1.7 Threat Origins*

While there are multiple threats to information security including natural disasters and systems failure, most threats have a human at their origin. We will focus on the threats with human origins.

Threats can be internal and external. Examples of external threats include experimenters and vandals, who are Amateur hackers, hactivists who have personal or political agendas, cybercriminals who are trying to make money, and information warriors who are professionals working for nation-states.

Despite the broad range of external threats, internal threats account for 80% of security problems according to the National Institute of Standards and Technology, or NIST. Internal threats can be intentional or unintentional and can include issues such as non-business use of computers which can allow threats in.

## *1.8 Types of Threats*

There are a broad range of information security threats. Some of the most common threats include website tampering, theft of data, denial-of-service attacks, and malicious code and viruses.

## *1.9 Website Tampering*

Website tampering can be a very big problem for your business. Website tampering can take many forms, including defacing your website, hacking your system, and compromising web pages to allow invisible code, which will attempt to download spyware to your computer.

Select each item to learn more.

## *1.10 Theft of Data*

Data theft also comes in several forms and the problems that come with data theft depend upon the kind of data that is stolen. Some examples of data theft include:

- Theft of computer files
- Inappropriate access to computer accounts
- Theft of laptops and computers
- Interception of emails or internet transactions
- Phishing emails that trick you into giving away personal information
- Spear phishing emails that deceive a specific group of people into responding
- Identity theft

## *1.11 Denial of Service Attacks*

A denial-of-service attack is an attack on a computer or website which locks the computer and/or crashes the system and results in stopped or slowed workflow, prevented communication, and halted eCommerce. Some common ways that attackers achieve denial-of-service attacks include:

- Volumetric attacks, which attempt to use all available bandwidth and slow or stop performance and
- TCP State-Exhaustion Attacks, which cause problems with things like firewalls and application servers

The ultimate goal of these attacks is always to prevent you from conducting business of any kind with your internet connected systems.

## *1.12 Malicious Code and Viruses*

Malicious Code and viruses may be some of the better-known threats. These threats send themselves over the internet to find and send your files, find and delete critical data, or lock up the computer or system. They can hide in programs or documents, make copies of themselves, and install themselves on your system to record keystrokes to send to collection point.

## *1.13 Reasons for Vulnerabilities*

All of the threats we have discussed can be very scary. Before we can address how to prevent attacks, we must first investigate the reasons that small businesses are vulnerable to these kinds of attacks.

- Computer hardware and software is outdated and/or insecure
- Poor or missing security policies that do not establish security protocols.
- Missing procedures for securing information
- Lazy oversight
- Loose enforcement of existing policies

## *1.14 Risk*

Let's talk for a moment about risk management, beginning with risk assessment. Risk assessment is the technique of assessing, minimizing, and preventing accidental loss to a business through the use of safety measures, insurance, etc. Removing all of the risk factors associated with attacks can be costly, but you need to ask yourself, "How much risk can I live with?"

Remember that no risk can be completely eliminated. If the consequence and probability of a breach is high, then your tolerance for risk is low. If the consequence is minor, more risk may be acceptable to you. If the risk is still too high after all protection efforts have been made, use commercial cyber insurance to "share" the risk/exposure. Contact your insurance provider to find out what options are available.

## *1.15 Protecting Yourself from Human Vulnerabilities*

The first step to protecting the information in your business is to establish security policies. It's very important that your security policies are comprehensive and up to date. You may have to revise your policies periodically as threats change. The second step to protecting information is ensuring that your employees both know ***and*** adhere to your security policies. Remember, most vulnerabilities have a human at their root!

## *1.16 Who Needs Training?*

Determine who will need to know the procedures. Consider:

- Employees who use computers in their work
- Help desk
- System administrators
- Managers/executives using specialized software
- System maintenance
- IT Out-sourcing

## *1.17 Training Basics*

You should train employees in basic security principles, and training should begin the first day at work. Include security policies and procedures, security threats and cautions, and basic security dos and don'ts in your training.

## *1.18 Continuing Education*

Training should continue with reminders and tools, including pamphlets, posters, newsletters, videos, rewards for good security, and periodic re-training - because people forget! Lack of training is one of the most significant information security weaknesses in most organizations.

## *1.19 Best Practices*

What should you actually train your employees on? How can you keep you information safe? You should address:

- Safe internet practices
- Safe email practices
- Safe desktop practices

## *1.20 Internet Practices*

Some best practices to keep in mind when it comes to the internet include:

- Do not surf the web with an administrative account
- Do not download software from unknown pages

- Do not download files from unknown sources
- Do not respond to popup windows requesting you to download drivers
- Do not allow any websites to install software on your computer
- Protect passwords, credit card numbers, and private information in web browsers and conduct online business and banking on secure connections

Password manager tools can help you keep track of secure passwords for each site.

## *1.21 Email Practices*

Some best practices to keep in mind when it comes to email include:

- Be careful when opening attachments
- Don't reply to unsolicited emails
- Don't click on links in an email

## *1.22 Desktop Practices*

Some desktop best practices include:

- Use separate computer accounts for each user
- Use passwords and don't share
- Use screen locking, log on and off, and power down your system at the end of the day
- Don't plug "lost" infected USB drives into systems
- Seriously consider encrypting sensitive data on your system. Try using your favorite search engine online to find encryption tools that will work within your computing environment.

Select blue items to learn more.

## *1.23 Protecting Your Systems*

Now let's discuss some ways to protect your information. There are several different areas you must consider in order to fully protect yourself.

## *1.24 Viruses, Spyware, Trojans, and Malware*

In order to protect yourself against viruses, spyware, trojans, and malware:

- Install anti-virus software
- Company-wide detection tools
- Company-wide process
- Assign responsibility in writing

- Up-to-date search definitions
- Include employee's home systems

21st century computers are complex and include mobile technology, tablets, and personal computers made by many different companies. These various systems tend to have different threats and often require different software in order to adequately protect against viruses, spyware, trojans, and malware. A basic understanding of your computer may help you protect it. Try searching for information about your particular system.

## *1.25 Hardware and Software*

Hardware and software protections require:

- Secure internet connection and change passwords
- Change passwords periodically
- Use software firewalls
- Patch operating systems and applications
- Secure wireless access points

## *1.26 Backup Procedures*

Some people don't consider how important backup procedures are for information security. Your goal should be the ability to restore systems and data to what existed before any threat is realized.

Make back-up copies of important information and restore weekly. Store a backup copy offsite for safe keeping. You should also test your backups to make sure that they actually work. Also keep in mind the importance of disposing of old computers and media securely. Just because you're finished with it doesn't mean someone else can't use it to get important information about you, your business, or your customers.

## *1.27 Summary*

That was a lot of information. In this course you have:

- Learned what cybersecurity is
- Learned why cybersecurity is important
- Learned about common cybersecurity threats and crimes
- Learned about risk assessment
- Learned what you can do to protect your business

## *1.28 Next Steps*

Now what should you do? Follow these steps to begin securing your business from cyber threats.

**Step 1.** Conduct an analysis of information security needs

**Step 2.** Assess the cost of losing your information

**Step 3.** Create a plan to protect your information

**Step 4.** Implement your plan through policies, training, and hardware and software controls

## *1.29 Resources*

SBA has a broad network of skilled counselors and business development specialists. Below is a short description of our resource partners:

- There are more than 1,000 **Small Business Development Centers** (SBDCs) located around the country. SBDCs provide management assistance to current and prospective small business owners.
- **SCORE** is a powerful source of free and confidential small business advice to help build your business. More than ten thousand SCORE volunteers are available to share their experience in lessons learned in small business.
- **Women's Business Centers** assist women and men in achieving their dreams by helping them start and run successful businesses. Some 90 WBCs are located around the country.
- SBA has over 60 **district offices** located throughout the country to help you start and grow your business.
- SBA's **Small Business Learning Center** is a powerful virtual campus with online training, videos, tools and links to local resources.

Find your local resource using our handy zip-code tool: www.sba.gov/local-assistance

There are additional cybersecurity resources you can access, including the National Institute of Standards and Technology, or NIST and the Department of Homeland Security (DHS). Most states have cybersecurity organizations as well.

## *1.30 Have a Question?*

Have a question?

- Call SBA - 1-800 U ASK SBA (1-800 827-5722)
- E-mail SBA - answerdesk@sba.gov
- Locate a SCORE counselor, SBA district office near you, or an SBDC office near you at www.sba.gov/local-assistance
- To provide feedback, comments or suggestions for other SBA online content, please use the following email: learning@sba.gov

## *1.31 Certificate*

Congratulations on completing this course.  We hope it was helpful and provided a good working knowledge on how to successfully protect your business from cyber-attacks. Click the certificate to receive a course completion confirmation from the US Small Business Administration.