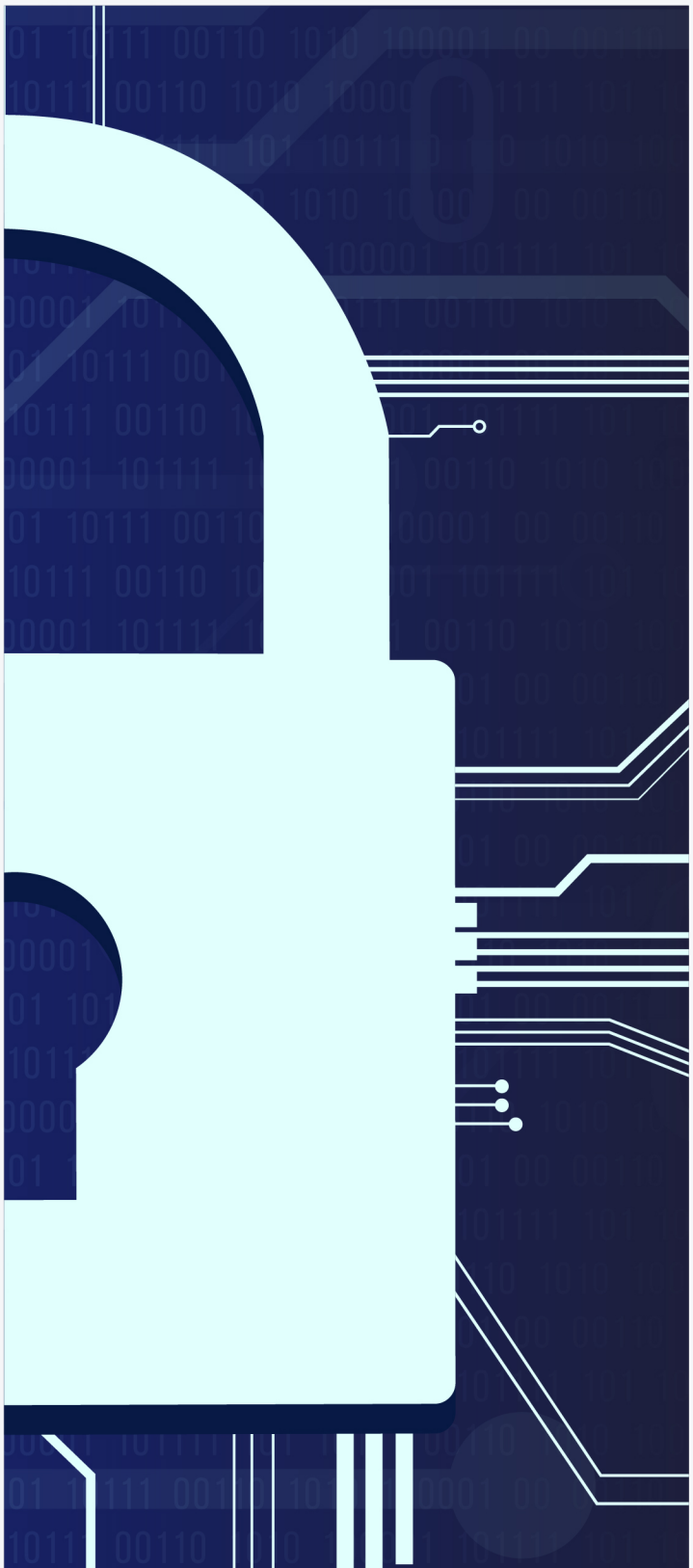
CYBER TRAINING

INSTRUCTION GUIDE

Presented By: Case Insurance Brokers Inc.

Contents

Introduction



This document is meant to supplement the Employee Cyber Training materials, and it is not meant for distribution to employees. This guide will walk you through the importance of cyber training for your employees, considerations that may be specific for your business and important topics to discuss with your employees.

As you read through this instruction guide, it is important to remember that employee cyber training should be customized to your business's unique needs and risks. For example, if your business has an online store, your risks will be substantially different than a business that only offers retail locations. Additionally, you may want to open the three employee training documents ("Overview & Best Practices," "Communication" and "Device Security") to consult as you read through this instruction guide.

Purpose

From the perspective of employees, training can often seem like one of the most monotonous tasks they can do. This is especially true when talking about cyber security, since your employees have likely been using computers, smartphones and other mobile devices for years without any negative consequences.

To ensure that employees are engaged in cyber security training, it's important to focus on the personal benefits of the training. **When employees are being trained, it's important to constantly emphasize that these measures are for both their personal and professional use.** For example, it can be difficult or next to impossible to get employees to use complicated, secure passwords to protect your business's information. However, if they learn hackers can access their personal financial accounts because they use weak passwords, and you give them tips to protect themselves, they will be much more likely to transfer those skills into a professional setting.

Training Preparation

Before training begins, it's important to read through the Cyber Employee Training Materials that you will give to your employees. As you read, be sure to familiarize yourself with all of the materials so you are prepared to answer any questions that your employees have. Also, don't be apprehensive about doing some research if you're unfamiliar with a subject—no one knows everything about cyber security.

To ensure that cyber training best fits the needs of your business and employees, you may want to focus on some topics more than others, and tailor them to your business's circumstances. For example, training could be vastly different if your business has an IT department to manage things like software updates and malware.

While you are going through the training materials, be sure to note what topics you would like to spend more or less time on. Then, by either editing the documents themselves or by taking notes, be sure to note any important steps employees need to take based on your business's unique circumstances.

The following is a general, but not comprehensive list, of the things you may want to consider including in your training documents.

QUESTIONS TO ASK BEFORE TRAINING OCCURS

Before training begins, here a few things you should consider:

- Who will be guiding the employees through the training? Does this person have a background in information technology (IT)? Does he or she have any other experience with cyber security?
- What format will be used during training (e.g., one-on-one sessions, a one-time meeting with multiple employees or weekly meetings)?
- What topics are most important to cover for your business?
- How will you know when employees have received an adequate amount of training? How will you determine that the training was effective or if more training is required?

Overview & Best Practices

SOFTWARE UPDATES

- Does your business have an IT department that will manage operating system (OS) updates and anti-virus software?
- Are your employees granted administrative permission on business devices that will allow them to update software?
- Are your employees allowed to use personal devices for business use? Do you encourage employees to regularly update these devices to get the latest security patches?

SAFE INTERNET BROWSING

- Do you specify which internet browsers your employees may use on business devices?
- Does your business block prohibited websites on business devices, or do you maintain a firewall that actively searches for vulnerabilities online and blocks employees who attempt to view them?

SECURE PASSWORDS

- Do you have criteria in place for password strength (e.g., including uppercase letters, numbers and/or special characters)?
- How often must employees change their passwords?
- Does your business have a policy regarding the use of password management systems?

NOTES: (START TYPING BELOW)

Overview & Best Practices

INSTALLING SOFTWARE

- What apps and programs are employees allowed to install on office computers? For example, can employees download and install things like Skype, Spotify, iTunes or computer games?
- Does your business's computers and other devices have guards in place to prevent employees from downloading prohibited software (e.g., not giving employees administrator privileges)?
- Are employees allowed to download apps onto mobile devices that your business owns? If so, what is the policy for purchasing these apps?

SOCIAL MEDIA

- Are employees allowed to view social media during the workday?
- Are employees allowed to view social media on business devices?
- Are employees allowed to make social media posts about work-related topics?

RECORD-KEEPING

- Are employees encouraged to print important records so they can be physically stored?
- Is physical storage a priority at your business? If so, are employees encouraged to delete digital records after they have been printed?
- Does your business use a cloud storage service or remote hard drive? What is the procedure for accessing remote files? How often is the service or hard drive checked to ensure that data isn't kept for longer than it should be? Do employees have access to cloud services or remote hard drives with business information on them?

NOTES: (START TYPING BELOW)

Communication

SOCIAL ENGINEERING

- Do all of your employees have access to a directory of employee information, including contact information? If so, do employees know to never share that information with anyone outside your company?
- Do employees use their personal email accounts for business use? Do you encourage employees to only use and trust work email addresses?
- Do employees know to double-check strange requests that might be part of social engineering with management first?

EMAIL

- Does your business use a unified email system? If so, does this system have a way to filter out unwanted emails, such as spam?
- Does your business have a policy for email best practices, such as verifying who sends an email and never clicking on links from an unknown source?

PHISHING AND SPEAR PHISHING

- Do your employees know not to send sensitive information electronically?
- Is your office set up in a way that employees can verify a request that's sent electronically? For example, by physically walking to a manager's office to double-check that a request is legitimate.

OTHER CYBER RISKS

- Would your employees feel comfortable approaching you or another authority figure for concerns relating to cyber security? If not, why?
- Is your business open to the public? How easy would it be for someone to walk into your office and blend in?
- Do you regularly check the credentials of people who walk into your office, or are they required to walk past a front desk?

NOTES: (START TYPING BELOW)

Device Security

WHO HAS ACCESS?

- Do your employees frequently take devices home with them? If so, do friends and family members have access to devices with business information on them?
- Do you require employees to password protect personal devices if they are used for business?

DEVICE SECURITY

- Do employees have easy access to other employees' computers or devices? If so, do you enforce a policy to lock devices when they aren't in use?
- Do you allow employees to use business devices in public areas?
- Are employees allowed to use business devices with unprotected or public Wi-Fi networks?

BUILDING SECURITY

- Do your employees know to question the presence of a stranger in the workplace?
- Are the doors and windows to your office locked, or do they require a key or password to enter?
- What are your building's operating hours? Is it possible to access the building outside these hours?
- If you have building vendors, have you contacted them to discuss any relevant cyber security provisions?
- Do you make employees aware when third-party vendors, such as maintenance and construction crews, will be at your workplace?
- Who has the keys to your office and all of its rooms? Is there a procedure to account for these keys, and to note when they're used?

NOTES: (START TYPING BELOW)

Device Security

PORTABLE MEDIA

- Does your business frequently use portable media such as hard drives, USB drives or flash drives? If so, are they password protected?
- Are employees aware that they should never plug in a portable media drive, unless they know exactly what is on it?
- Are employees allowed to bring in and use their own portable media drives?

TRAVEL

- Do your employees frequently travel with devices owned by your business?
- Are employees allowed—or even capable of using—unsecured or public Wi-Fi networks?
- Do your employees know not to leave devices in an unsecure or dangerous area? This also includes extreme temperatures, such as not leaving a laptop in a locked car on a hot or cold day.

NOTES: (START TYPING BELOW)

How to Conduct Training

Once you have determined how training will take place and gone through the training documents and tailored them to your business, you are ready to conduct training. While you are introducing employees to cyber training, you may want to bring up these topics:

- Be sure to emphasize that employees are there for their personal benefit, and that the training is intended to make their own personal information, as well as your business's, more secure.
- If you are conducting training in response to a specific incident, you may want to have a conversation with employees about the specifics regarding the incident.
- Explain to employees that the training is also meant to make sure that everyone understands your business's policies. And, even though everyone will make mistakes from time to time, employees should approach a manager or the IT department (if applicable) if they believe they or another employee has inadvertently or purposefully violated your policies.
- Encourage your employees to take notes during training.
- Be sure to ask your employees if they have any questions before training begins, and encourage them to ask questions during training. When you answer questions, it's extremely important to be honest if you don't know the answer. Instead, do your best to find the answer when you can, and get back to your employees as soon as you can with the answer.