|  |  |
| --- | --- |
| Healthcare, Inc.  Learning Objectives |  |

Contents

[Overview 2](#_Toc483992817)

[Topic 1: PCI Compliance 2](#_Toc483992818)

[Target Group 2](#_Toc483992819)

[Goal 2](#_Toc483992820)

[Background 2](#_Toc483992821)

[Learning Objectives 2](#_Toc483992822)

[Topic 2: Phishing 6](#_Toc483992823)

[Target Group 6](#_Toc483992824)

[Goal 6](#_Toc483992825)

[Background 6](#_Toc483992826)

[Learning Objectives 6](#_Toc483992827)

[Topic 3: Encryption 8](#_Toc483992828)

[Target Group 8](#_Toc483992829)

[Goal 8](#_Toc483992830)

[Background 8](#_Toc483992831)

[Learning Objectives 8](#_Toc483992832)

# Overview

The learning objectives are the specific behaviors that will reduce risk to Healthcare, Inc. Each objective will include Progress and Impact Metrics. The Progress Metric is the method for ensuring the correct behavior was understood by the learner. The Impact Metric is the method for measuring the effectiveness of the desired behavior change.

# Topic 1: PCI Compliance

## Target Group

Organization-wide employees are required to have PCI training. In addition, the Finance and Operation departments have direct interaction with the cardholder data environment and requires additional training.

## Goal

To make all personnel aware of the cardholder data security policy and procedures.

## Background

Healthcare, Inc. processes payment cards online, over the phone, or via facsimile. In order to limit liabilities, we must annually attest to compliance with PCI DSS. A formal Security Awareness Program must be established to comply with PCI requirement 12.6. The program must include multiple communication methods, verify employees receive training upon hire and annually thereafter, and employees must acknowledge annually they have read and understood the security policy and procedures.

## Learning Objectives

|  |  |
| --- | --- |
| PCI Compliance | |
| Learning Objective 1 | Learner can identify cardholder data that is allowed to be stored. |
| Progress Metric | Learner can correctly identify or match at least 3 of 4 data elements permitted for retention from a list of all cardholder data elements. |
| Impact Metric | The number of files matching string searches of restricted cardholder data across the organization’s systems. |
| Learning Objective 2 | Learner can identify when transmission of cardholder data requires encryption. |
| Progress Metric | Learner can correctly determine if cardholder data should be encrypted given a network transmission scenario. |
| Impact Metric | A sampling of outbound network connections are inspected for unencrypted cardholder data. |
| Learning Objective 3 | Learner can identify the antivirus software is enabled. |
| Progress Metric | Learner can correctly select 2 methods to identify antivirus is running and is enabled. |
| Impact Metric | A sampling of systems are inspected to determine if antivirus software is running and is enabled. |
| Learning Objective 3 | Learner can identity the process for granting access to cardholder data. |
| Progress Metric | Learner can select the correct process to grant cardholder data access from a list of 3 other false processes. |
| Impact Metric | A sample of accounts with cardholder data access will be verified. |
| Learning Objective 4 | Learner can explain the appropriate method for disposing of printed documents containing cardholder data. |
| Progress Metric | Learner can select the correct process for paper destruction of confidential information from a list of 3 other false processes. |
| Impact Metric | A sample of trash bins are searched for documents with confidential data. |

|  |  |
| --- | --- |
| PCI Compliance – Operations | |
| Learning Objective 1 | Learner can explain the change management process for firewall and network architecture. |
| Progress Metric | Learner can identify the correct process for making a firewall change among 3 other false processes. |
| Impact Metric | Determine if each firewall rule, outside of the baseline, has an appropriate change management record. |
| Learning Objective 2 | Learner can explain the patch management process. |
| Progress Metric | Learner can match the correct process for applying operating system patch among 3 other false processes. |
| Impact Metric | Compare the number of uninstalled operating system patches to the number of available patches for each system. |
| Learning Objective 4 | Learner can follow the code review process before submitting new code for approval. |
| Progress Metric | Learner can identify the correct code review process among 3 other false processes. |
| Impact Metric | For a sample of coding changes, review change management records to determine if a different developer or manger acknowledged review of the code before it was approved. |
| Learning Objective 4 | Learner knows only sample data is to be used in development environments. |
| Progress Metric | Learner can identify or match sample cardholder data. |
| Impact Metric | Sample testing data and compare with production data to identify any matches. |
| Learning Objective 5 | Learner can explain what a test account is and knows test accounts are not used in production environments. |
| Progress Metric | Learner can identify the common test account names used by the organization. |
| Impact Metric | Search for test account names in the production cardholder data store. |
| Learning Objective 6 | Learner can identify injection flaws. |
| Progress Metric | Learner can select the correct code that would permit an injection flaw. |
| Impact Metric | Static code or third party testing of the application to identify injection flaws. |
| Learning Objective 7 | Learner can identify buffer overflows. |
| Progress Metric | Learner can select the correct code that would permit a buffer overflow flaw. |
| Impact Metric | Static code or third party testing of the web application to identify buffer overflow flaws. |
| Learning Objective 8 | Learner can identify strong cryptographic functions. |
| Progress Metric | Learner can select or match the strong cryptographic functions from a list of 6 functions. |
| Impact Metric | Determine the number of weak cryptographic functions used in production code. |
| Learning Objective 9 | Learner can identify secure communications methods. |
| Progress Metric | Learner can select or match the secure communication methods from a list of 4 methods. |
| Impact Metric | Determine the number of insecure communications channels in use on each system. |
| Learning Objective 10 | Learner can identify generic error messages. |
| Progress Metric | Learner can select a generic error message from a list with 3 other non-generic messages. |
| Impact Metric | Force error message generation in the application and record the number of messages that are not generic. |
| Learning Objective 11 | Learner can identify cross-site scripting flaws. |
| Progress Metric | Leaner can select the correct code that would permit a cross-site scripting flaw. |
| Impact Metric | Static code or third party testing of the application to identify cross-site scripting flaws. |
| Learning Objective 12 | Learner can identify improper access control. |
| Progress Metric | Learner can select or match the types of insecure access control from a list of 6. |
| Impact Metric | Third party testing or audit of access to application objects or functions. |
| Learning Objective 13 | Learner can identify cross-site request forgery. |
| Progress Metric | Learner can select the correct coding technique that would produce cross-site request forgery flaws. |
| Impact Metric | Third party testing or internal audit of applications to determine if cross-site request forgery flaws exist. |
| Learning Objective 14 | Learner can identify secure authentication and session management techniques. |
| Progress Metric | Learner can select the correct authentication and session management methods that are secure. |
| Impact Metric | Third party testing or internal audit of applications to determine if insecure authentication or session management methods exist. |

# Topic 2: Phishing

## Target Group

Organization-wide employees will be offered instructor-led training on threats coming from phishing email messages. Phishing can have a higher impact on the Finance department as they process vendors’ payments.

## Goal

To make personnel aware of threats from phishing messages and the appropriate responses to them.

## Background

Phishing attacks are the primary method attackers are using to gain initial access to an organization’s systems. Email messages with attached documents containing malicious code can directly infect computers when employees fall victim. Other messages may contain links to malicious websites designed to steal a victims credentials or infect their computer through web browsers.

## Learning Objectives

|  |  |
| --- | --- |
| Phishing | |
| Learning Objective 1 | Learner can explain the clues that identity phishing messages. |
| Progress Metric | Learner can correctly identify at least 2 indicators in a sample phishing messages. |
| Impact Metric | Number of messages reported as phishing to the security team. |
| Learning Objective 2 | Learner knows how to report suspicious email messages. |
| Progress Metric | Learner can correctly select the contact address to report phishing messages from a list of 3 other false contact addresses. |
| Impact Metric | Number of messages received at the phishing contact address. |
| Learning Objective 3 | Learner can identify phishing messages with a pretext from an authority position. |
| Progress Metric | Learner can select the correct phishing message from examples of 3 email messages. |
| Impact Metric | Number of reported messages that are actually phishing messages. |
| Learning Objective 4 | Learner can identify phishing messages with a pretext requiring an immediate response. |
| Progress Metric | Learner can select the correct phishing messages from examples of 3 email messages. |
| Impact Metric | Number of reported messages that are actually phishing messages. |
| Learning Objective 5 | Learner can identify phishing messages with a pretext for a missed package or prize. |
| Progress Metric | Learner can select the correct phishing messages from examples of 3 email messages. |
| Impact Metric | Number of reported messages that are actually phishing messages. |
| Learning Objective 6 | Learner can identify the impact of opening attachments in a suspicious email message. |
| Progress Metric | Learner can correctly select at least 3 results of opening a malicious attachment in a phishing email from a list of 6. |
| Impact Metric | Number of files quarantined by antivirus that were received from an email message. |
| Learning Objective 7 | Learner can identify the impact of clicking links in a suspicious email message. |
| Progress Metric | Learner can correctly select at least 3 results of clicking a malicious link in a phishing message. |
| Impact Metric | Number of malicious links prevented by URL filtering that were received from an email message. |

# Topic 3: Encryption

## Target Group

Organization-wide employees, Finance and Operation departments will be offered instructor-led training on encryption.

## Goal

To make personnel aware of the type data that needs to be encrypted and when to encrypt it.

## Background

Encryption is used to protect the confidentiality of information sent across networks or stored on media. If secure cryptography functions are not used, attackers can easily compromise encryption without the knowledge of the sender or receiver. With correct key management, encryption can be used as another access control. Misplaced or stolen storage media has been a frequent cause of breach notifications for companies in the past.

## Learning Objectives

|  |  |
| --- | --- |
| Encryption | |
| Learning Objective 1 | Learner can explain differences in encryption use. |
| Progress Metric | Learner can identity the correct encryption for two different use cases. |
| Impact Metric | None. |
| Learning Objective 2 | Learner can identify when a website is using an appropriate encryption. |
| Progress Metric | Learner can select the website using encryption from screenshots of 2 websites. |
| Impact Metric | None. |
| Learning Objective 3 | Learner can explain what data needs to be encrypted. |
| Progress Metric | Learner can identify confidential data in a list of 6 other non-sensitive data. |
| Impact Metric | Number of incidents reported of lost or stolen data in clear text. |
| Learning Objective 4 | Learner can explain how to encrypt data in an email. |
| Progress Metric | Learner can select the correct method for encrypting an email message. |
| Impact Metric | Number of incidents reported where clear text data was lost or stolen. |
| Learning Objective 5 | Learner can explain the importance of keeping encryption keys secure. |
| Progress Metric | Learner can select the correct key storage methods. |
| Impact Metric | Number of employees with access to encryption keys. |