PCI-DSS COMPLIANCE REPORT

Sample engineering company with 200 employees

safetica®

Content

The Payment Card Industry Data Security Standard . . . 3

Incidents per reported period . . . 3

Identifying Sensitive Data . . . 4

Defining Data Channels . . . 4

Top 3 PCI-DSS sensivite information files channels . . . 5

Maintaining Channel Control . . . 5

Encrypting Hard Drives . . . 8

Endpoint Overview . . . 8

Critical Applications Access . . . 9

Visiting Critical Websites . . . 9

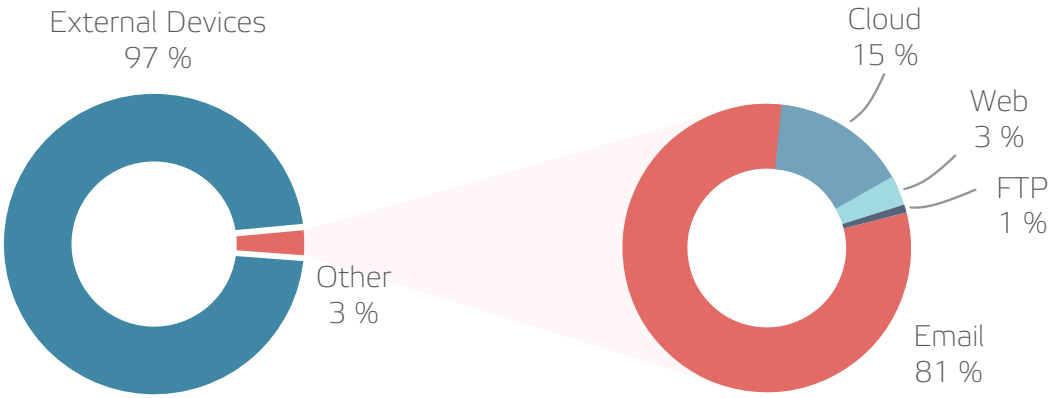
The Payment Card Industry Data Security Standard

The Payment Card Industry Data Security Standard (PCI-DSS) is a standard developed to protect sensitive data concerning payment cards and data created by using such cards. The standard itself consists of twelve requirements which are further divided into sections. To achieve full compliance with the PCI-DSS, a company must fulfill all the requirements stated in these sections. Currently, version 3.2 of PCI-DSS, released in April 2016, is in use.

All information about credit card numbers, payments and card holders' data is, according to this document, further cited as "PCI-DSS sensitive information".

Information provided in this report is mainly focused on PCI-DSS regulation requirements. Additionally, general recommendations which will help you to secure your environment and improve global security can also be found here.

Incidents per reported period



15 Regulatory compliance: suspicious file uploads

32 Users with security incidents

Incidents per file

company_contacts.doc . . . . . 10×
unit_blueprint.dwg . . . . . 6×
customer_data.xls . . . . . 2×

Major findings

⚠ 5,128 files containing PCI-DSS sensitive information

⚠ 2,791 out of 13,741 emails contained PCI-DSS sensitive information

⚠ Only 25 out of 280 devices used in the environment are encrypted

Identifying Sensitive Data

According to PCI-DSS requirements you are obliged to protect stored cardholder data.

⚠ 5,128 files containing PCI-DSS sensitive information

Effective data protection can only be applied if you know where the sensitive content is located. The first step is to find all the files containing PCI-DSS sensitive information, classify it as sensitive and set up the best ways to handle it.

Findings:

- These files are stored on both local disks and network share drives
- In total, 12 out of 200 users have these files on their local disks
- Examples of these locations are:
  - *\\192.168.91.151\operations*
  - *\\192.168.91.142\archives*
  - *C:\Users\l.baker\Desktop*

Recommended Settings in Safetica

- Classify sensitive data in *Safetica Console > DLP > File Tagging > Content rules*
- Create security policies in *Safetica Console > DLP > DLP rules*

Defining Data Channels

According to PCI-DSS requirements there is a need to track and monitor all network channels.

⚠ Over 33,000 files containing PCI-DSS sensitive information found in diverse channels

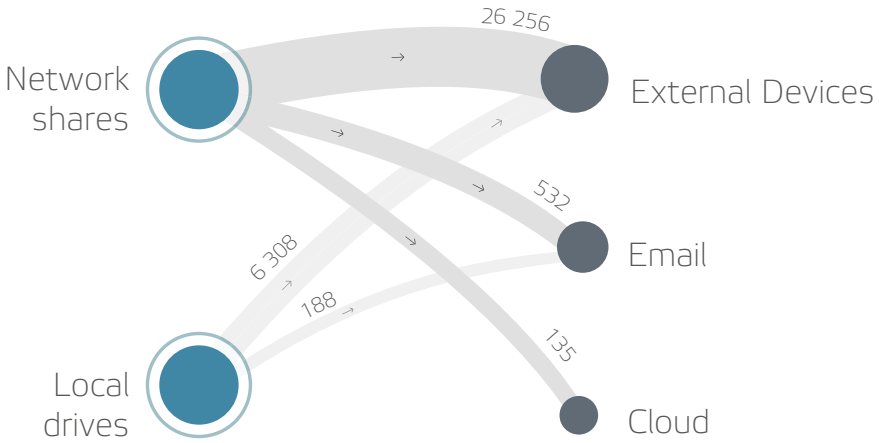
To be able to protect sensitive data it is essential to know what happens with it. Once you know exactly how it flows, you can set up procedures to ensure it stays within the company environment.

Findings:

Overview of files with PCI-DSS sensitive information by channel:

- 32,564 files were copied to external devices
- 720 files were sent via email
- 135 files were uploaded to Cloud services such as OneDrive for Business, OneDrive Personal, SharePoint and Dropbox
- 30 files were uploaded via Web browsers to different file storage services and social networks
- 8 files were transferred via FTP

Top 3 PCI-DSS sensitive information files channels:



Recommended Settings in Safetica

- Proceed with the Analysis of internal data security

Maintaining Channel Control

According to PCI-DSS requirements it is mandatory to develop and maintain secure systems and applications, restrict access to cardholder data and protect the transmission of such data across networks.

Uploading to Cloud Services

The usage of cloud storage registered on 56 computers in the company

Using public cloud storage such as Dropbox, OneDrive or Google Drive instead of an official company cloud service represents another possible way of leaking PCI-DSS sensitive information. To prevent this, it is advisable to identify the use of public cloud storage as well as prohibit it.

Findings:

- Dropbox sync folder is used on 12 computers
- OneDrive Personal is globally allowed even though OneDrive for Business is available
- 15 files containing PCI-DSS sensitive information transferred to cloud drives

Recommended Settings in Safetica

- Identify the usage of public cloud storage across the whole company environment in *Safetica Console > DLP > Disk guard*
- Restrict the upload of files only to official cloud storage in *Safetica Console > DLP > Channel Control or Safetica Console > DLP > DLP rules*

Sending Sensitive Data via Email

⚠ 2,791 out of 13,741 emails contained PCI-DSS sensitive information

The unrestricted ability to send files with PCI-DSS sensitive information via email may also potentially result in leaked data.

Findings:

- 17 users sent files with PCI-DSS sensitive information by email
- Messages were sent to a total of 45 recipients
- 1,371 out of 2,791 emails containing PCI-DSS sensitive information were sent outside of the corporate domain

Recommended Settings in Safetica

- Forbid files containing PCI-DSS sensitive information to be sent outside of the company in *Safetica Console > DLP > Channel Control or Safetica Console > DLP > DLP rules*

Uploading to Public Websites

⚠ The usage of WeTransfer.com registered in the company

Another way files containing PCI-DSS sensitive information can leave the company is through websites such as WeTransfer.com, MEGA.nz or facebook.com.

Findings:

- 13 users uploaded files with PCI-DSS sensitive information to public websites
- 30 files containing credit card data were uploaded to websites
- In total, users uploaded files to 7 different public websites

Recommended Settings in Safetica

- Forbid files with PCI-DSS sensitive information to be uploaded outside the allowed websites in *Safetica Console > DLP > Channel Control or Safetica Console > DLP > DLP rules*

Bringing One´s Own Device

⚠ Only 25 out of 280 devices used in the environment are encrypted

Files containing PCI-DSS sensitive information can be accidentally or intentionally transferred to unprotected devices and taken out of the company.

Findings:

- 5,264 files containing sensitive data were copied from a network path to an external device
- 51 users connected their mobile phones or other Windows Portable Devices
- Only 173 out of 213 endpoint stations are protected by Safetica

Recommended Settings in Safetica

- Limit the use of external devices by setting a list of permitted devices in *Safetica Console > DLP > Device Control using Zones*
- Identify and prohibit moving and copying files containing PCI-DSS sensitive information to unencrypted devices
- Install Safetica Client on all computers in the network in *Safetica Console > Maintenance > Update and deploy*

Using Instant Messaging Applications

⚠ The usage of Instant Messaging Applications registered in the company

Using instant messaging applications such as Skype or Slack can also be a leak source for files containing PCI-DSS sensitive information.

Findings:

- Skype is globally allowed even though Skype for Business is installed
- 273 sensitive files were sent through Skype
- 23 sensitive messages were shared using Slack

Recommended Settings in Safetica

- Forbid files containing PCI-DSS sensitive information from being sent via Instant Messaging applications in *Safetica Console > DLP > Channel Control*

Encrypting Hard Drives

According to PCI-DSS requirements, it is necessary to encrypt data and drives across platforms.

⚠ Only 25 out of 560 hard drives in the company are encrypted

To protect PCI-DSS sensitive information, we recommend that all in-use company hard drives be encrypted.

Findings:

- Only 25 out of 560 computer drives are encrypted using BitLocker
- 34 computer drives are encrypted with a different encryption method
- There is no policy for encrypting external devices

ⓘ **Recommended Settings in Safetica**

- Encrypt all hard drives so that they can only be opened by authorized users in *Safetica Console > DLP > BitLocker disks*

Endpoint Overview

According to PCI-DSS requirements, regular process and security tests should be performed.

⚠ 13 endpoint devices running with Windows XP or Vista operating systems

Using an outdated operating system represents a significant security threat. Such devices can easily become an entry point for hackers to break into the company computer system.

Findings:

- There are 8 computers with Windows XP installed
- There are 5 computers with Windows Vista installed
- Only 173 out of 213 endpoint stations are protected by Safetica

ⓘ **Recommended Settings in Safetica**

- Identify endpoint devices running on outdated or unsupported operating system in *Safetica Console > Maintenance > Endpoint management*

Critical Applications Access

According to PCI-DSS requirements, all access to system components must be identified and authenticated as well as protected against malware.

⚠ 5 suspicious applications launched

Untrained users, especially, can easily run critical applications that can infect the company environment with malware or other dangerous software.

Findings:

- 2 users ran a critical type of application, e.g. a Keylogger
- File hosting servers are globally allowed in the environment, and can be used freely
- 5 users used torrent applications to download data

Recommended Settings in Safetica

- Block access to suspicious websites in *Safetica Console > Supervisor > Application control*
- Set Informative or Security Alerts in *Safetica Console > Alerts*
- Set overview reports to be sent to management in *Safetica Console > Reports*

Visiting Critical Websites

According to PCI-DSS requirements, install and maintain firewall configuration to protect cardholder data and the environment.

⚠ 32 suspicious websites visited

Visiting suspicious websites is another way the company environment can become infected by dangerous software.

Findings:

- 13 users accessed websites from the critical categories Pornography, Illegal or Malware
- File hosting servers are globally allowed in the environment, and can be used freely
- WeTransfer service was accessed regularly multiple times

Recommended Settings in Safetica

- Block access to suspicious websites in *Safetica Console > Supervisor > Web control*
- Set Informative or Security Alerts in *Safetica Console > Alerts*
- Set overview reports to be sent to management in *Safetica Console > Reports*