**Case Study Preliminary Information:**

* Each scenario represents a bank branch and its infrastructure
* ISP (A) is different than ISP (B) and ISP (C). There are 3 different ISPs
* ISP (B) is a back-up ISP, the corporate network gets automatically switched to this ISP if the main ISP(A) fails
* Instant issue is a printer that prints debit cards with a Visa/MasterCard logo
* Instant issue only receives credit card information from the vendor via a peer to peer secure VPN connection. The Instant Issue prints the card using the information received from the vendor
* Cash Advance is a machine used to obtain cash from credit cards (not issued by the bank). The credit card is read by the machine and the information is sent to the vendor who processes the credit card information, returning an approval/denial for the cash advance
* The Cash Advance is connected via SSL/TLS 1.0
* The wireless access point is for guest use – it is not password protected and communications are not encrypted
* The bank does not process credit card information

**Background:**

The bank is designing a “branch of the future” layout and has reached out to the Information Security Department to help determine the safest architecture. Currently the Cash Advance machines communicate with the vendor using POTs lines. None of the branches actually have a wireless AP yet, and the Instant issue is the only resource on ISP(C).

The IT department wants to know which one of the two solutions they should select. Your job is to understand the need, evaluate the possible solutions, and provide IT with the risks of each, compliance requirements and recommendations.

**Questions:**

1. Are there PCI DSS requirements for the Cash Advance machine?

Yes, always as it processes the credit card information and communicates with the vendor and server. The requirements would be as follows:

**Requirement 3**: We need to protect the data of the cardholder who tries to access the machine even though we don’t store the data permanently.

**Requirement 4**: Protecting the data during transmit is very important as in this case they are using TLS 1.0 which is outdated and updating the transmission protocol to TLS 1.2 or higher is better encryption of the data.

**Requirement 10**: Ensure we have enough logs to investigate and monitor the access to credit card data for better accountability.

1. Are there PCI DSS requirements for the instant issue printer which only handles debit card information?

The answer to this is yes because PCI DSS also applies to the instant issue printer because it processes card data via a secure peer-to-peer VPN connection so it comes under PCI DSS requirements as follows:

**Requirement 1**: We must ensure that the network configurations are secure and we have a firewall and strict rules in place for the VPN connection.

**Requirement 4**: No matter what we need to protect the data and logs at transmission.

1. Does scenario A require both networks to be PCI compliant? Explain your answer

The first scenario is almost perfect and interesting. I think Scenario A doesn’t require PCI compliance on both networks as the guest wireless is completely isolated from the corporate network and doesn’t handle the cardholder data.

We need to secure the network that handles the Instant Issue printer and the cash advance machine for the following reasons:

1. The wireless network is open as it is not password protected and doesn’t transmit the data of the cardholder data.

2. ISP (c) which is connected with Instant issue and cash advance machine on the one side and transmitting and storing of the card data on the other end. So this network must completely comply with PCI DSS.

1. Does scenario B require both networks to be PCI compliant? Explain your answer

The second scenario is completely involving both networks as it is using backup ISP (b) which introduces shared infrastructure, including the systems what handles the sensitive credit card data and the guest network which is not encrypted or protected through password. The concerns we have regarding this scenario are as follows:

1. Exposure of the backup network because of integration of the backup server.

2. PCI DSS should be compliant because SSL/TLS 1.0 which is used in the Cash Advance machine should be updated to 1.2 version or higher for better protection while the data at transit.

3. Proper segmentation between the servers handling the card holder data and not using the data as it can possibly put the corporate network on danger.

1. If you answered yes to questions 3 and/or 4:
   1. Determine which IT resources need to be PCI DSS compliant for each scenario and why

Scenario 1:

**Cash Advance Machine**: Uses and transmits data using TLS 1.0 should be updated to TLS 1.2 or higher.

**Instant issue printer**: It uses a VPN for handling the cardholder data.

**Firewall**: It stops the threat to corporate networks and ISP (c) as well.

**Switches and ISP (c)**: Better and secure transmission of data and isolation from other networks involving corporate data.

Scenario 2:

Same for all the devices in scenario 1 but not limited to the following devices.

**Backup ISP (b)**: As it handles the cardholder data like helps to connect to systems and transmit it.

**Switches and Segmentation**: We should ensure the proper separation of guest network traffic from CDE.

* 1. Determine which questionnaire category each solution should be under. Include a link to each questionnaire.

Scenario 1:

**Cash Advance Machine**: For standalone termination connection through IP (SAQ B-IP).

**Instant Issue Printer**: For storing, processing, and transmitting the cardholder data (SAQ D).

1. Which solution generates more risk and why?

It is clear from both scenarios that Scenario B is more risky for the following reasons:

1. **The Backup ISP (b)** connects the guest network with the corporate network creating a possibility of lateral movement if an attacker gets access to the guest network as it is not protected.

2. The significant vulnerability of using TLS 1.0 which could potentially be broken and a chance of data exposure and data manipulation.

3. Also monitoring and keep tracking of logs for both networks increases the cost and chances of misconfigurations and breaches.

1. Is there a third solution that has less PCI DSS requirements? If so, create a diagram of it.

We can minimize the PCI DSS requirements through network segmentation and network policies and offloading certain cardholder data responsibilities to vendors. We can make the following changes.

1. **Managing payment through vendor**: Giving whole handling to vendors like credit card transaction processing making the machines work as thin clients so that there will be no need to store data locally.

2. **Tokenization of Cardholder data**: Replacing the credit card data with tokens on Instant issue printer and Cash advance machine will highly reduce the risk of storing sensitive cardholder data. It is effective in reducing the PCI DSS.

3. **Isolated network for PCI Systems**: Maintain the separation and overlap between guest and corporate networks as much as possible and make sure of separate handling for the network involving the Instant Issue Printer and Cash Advance machine.

4. Good separation between the Access point handling wireless network and PCI network.

5. Upgrade the protocols and algorithms to the latest version like TLS 1.2 or higher and a good encryption algorithm for storing the tokens on rest like AES-256.

A diagram of a cloud computing network

Description automatically generated

As mentioned before, in this scenario, the corporation does not handle credit card information and only the vendor has access to it. The printer uses a VPN and the cash advance uses the latest SSL/TLS and are both in separate networks protected by a firewall. This is due to the PCI-DSS network being isolated from other networks and can be secured more easily.

1. Let us know how long it took you to complete this Case Study. Thank you!

The case study took about 2 days to complete.