By: Dylan Thomas and Alex Gudgel

Texas Roadhouse SecUrity

**Table of Contents**

Executive Summary p. 3-4

PCI DSS Compliance p. 5-8

IT Backup and Restore p. 8-10

Training p. 10-11

Technical Security p. 12-14

Physical Security p. 14-16

Work Cited p. 17

**Executive Summary**

We are going to discuss the information security infrastructure of Texas Roadhouse (TR). Some areas of interest are PCI DSS Compliance, Backup and Restore, Training, Technical Security, and Physical Security.

In terms of PCI DSS compliance we are going to talk about certain policies that help uphold PCI DSS compliance. For example, IT cardholder data security policy and IT wireless security policy. I am going to talk about how to improve these policies to make PCI DSS a smoother process than before. The less time the auditor takes to review, the better.

Backup and Restore, if all system are down, a restore of all systems will take place at their offsite data center. Backup tapes, SAN copy, WAN Aggregator, secondary firewall and other replication solutions would be used to bring their production systems back online at the offsite data center. There is room for improvement in terms of using the cloud to backup and restore the data.

Training, employees are trained at the corporate office as well as in the stores to help improve data security. In the corporate office and in the restaurants, they greatly stress to inform the security team of any suspicious activity. I’ve noticed they need to improve employee awareness of security risks. They also need to improve training their employees at their store locations on checking terminals for tampering, not writing down cardholder information, and to keep the back of house door locked to protect computers.

Technical Security, Texas Roadhouse uses an IPsec VPN tunnel which allows a secure connection from the stores and back to corporate. This allows the corporate headquarters to communicate with the terminals and back of house computers remotely. They also use anti-virus and anti-malware software to prevent threats. Texas Roadhouse is having issues incorporating two factor authentications because the firewalls can't handle the overhead. Also, Texas Roadhouse has password requirements at their headquarters but not for their back of the house store computers. Managers can make their passwords anything they choose, this is something we recommend them changing. We recommend them having a password dictionary and a requirement of eight letters, at least one number, at least one capital and lowercase letter, and at least one special character. We also recommend them to use SD-WAN cloud networking to allow them to monitor their network easier and incorporate two factor authentications.

Physical Security, they use a key card system at the corporate office to access the stairs, elevator, and each department on every floor. Their need for improvement would be at the stores. Access to the back of house computers is only protected by one door with a single key. This is where all the cardholder data can be accessed. Most of the time the doors leading outside are propped open which is a vulnerability. An alarm system should be implemented to go off if the door leading outside is open for too long. Also, key cards should be used as well as a key to unlock the door handle.

**PCI DSS Compliance**

Texas Roadhouse must be compliant with the Payment Cardholder Industry Data Security Standard (PCI DSS) because they process mass amounts of cardholder data when customers purchase meals at the restaurants. PCI DSS is a yearly audit that takes a 3-5-month process for completion. This section is mainly discussing policies that are put in place to comply with PCI DSS and we are discussing how we can improve those policies. I will get more in depth with the technical and physical side of security in later sections.

To get started, certain policies are upheld at the restaurants to make sure that they are compliant with PCI DSS. One of those policies is the IT Cardholder Data Security Policy. Certain standards mentioned in the policy are Texas Roadhouse will run background checks on all employees that are hired or change to a different job task. Those job tasks include: Manager roles (5 different roles), Local Store Marketer, Store Admin, and Key Hourly employees [3].

Texas Roadhouse upholds physical media protection requirements such as, hard copies of cardholder data are not permitted. Any physical media with cardholder data must be labeled and monitored as confidential information. If it is being sent outside of Texas Roadhouse then it must be logged and transported by a delivery method that can be traced. If it is stored physical media with cardholder data then it must be inventoried at least annually to ensure nothing is lost and possibly in the wrong hands. Once the physical media with cardholder data is no longer needed then it must be destroyed in a way that is unrecoverable [3]. For example, hardcopy materials and hard drives must be disposed of in the proper way to ensure no one can get their hands on pieces that could be restored. Just throwing it in the dumpster has risks due to people dumpster diving to gain access to confidential information. That is why a third party is used to properly dispose of the physical cardholder data.

The most important section mentions how long the data is stored and secure while accessible over the network. This includes cardholder data being keep for 7 days after the transaction. Transaction data for a single day is keep for 53 additional days in hashed format. AES 256-bit encryption is used to encrypt the cardholder data that is processed through a transaction. The encryption key is dynamic meaning it changes over time and because of this there is no need for key management. To ensure protection on the display of the point of sale (POS) terminals, only the last 4 digits of the permanent account number are displayed or printed. If someone needs the data after a transaction has been completed then you must inform IT store help desk staff [3].

Texas Roadhouse could improve on this policy by providing a separate policy for the physical media protection and disposal. You could add to the physical media protection by mentioning where the physical media is stored and secured at the corporate office. This would insure the auditor that the physical media won’t end up in wrong hands who is not authorized to handle the physical media with cardholder data.

A separate policy for employment would be necessary for the mentioning of background checks on all employees who work at the stores. Also, you could mention other topics like hostile and friendly departure procedures, employment contracts that are created after an employee accepts a job offer, new hire orientation procedures where an employee is introduced to the culture and flow of the organization [5].

This would allow you to focus more on how the cardholder data is encrypted (AES 256-bit) but go more in depth with other encryption techniques. For example, how the cardholder data is transmitted over a network with IPSec encryption.

Another important policy to comply with PCI DSS and keep the cardholder data secure is the Wireless Security Policy. Major topics in this policy are the security of wireless access points. Wireless access points are never to be placed in the Texas Roadhouse cardholder data environment meaning placed in the store locations, without the prior approval from IT management. To further ensure this does not occur, stores are inspected each quarter by the managing partner who looks throughout the store to check for rogue access points. If an access point attempts to spoof a TR SSID or MAC address to where it would become a rogue access point, an alert is generated and sent to the log management system [4].

The wireless access points are configured with user authentication on all management and administrative interfaces enabled on the devices and devices can only be updated or changes over a wired connection. Most importantly, the wireless access points must keep a point to point encryption between the access points and devices connected to the store network at all times [4].

This policy could be improved by separating how the wireless access points are managed at the corporate office and in the restaurants. Corporate is not in the PCI DSS scope because the wireless access points are not involved with cardholder data. It would still benefit the auditor in knowing how security is upheld on the wireless access points in the corporate office, this would ensure they are not in the cardholder data scope. Its beneficial for the auditor to know the employee Wi-Fi is secured using WPA2 encryption and how the laptops and desktops at corporate can only connect to the employee Wi-Fi if they are under the Texas Roadhouse domain. These are all good topics to mention about the corporate side of wireless access points. You would not want any computer to be able to connect to the employee Wi-Fi and gain access to file servers with confidential information.

Another topic to mention would be how the corporate office is checked for rogue access points so no employee connects to the wrong access point. This would give the attacker the option to monitor everything that person is doing over the internet.

**IT Backup and Restore**

Texas Roadhouse backs up their data on tapes. Once the tapes in the data center are full, the tapes are sent to an offsite location where they are stored. Texas Roadhouse has daily incremental backups of production data that occur nightly. They do full backups of production data on a weekly basis. System backups of all servers are performed every weekend. Texas Roadhouse keeps backup logs and have automated emails to inform information security professionals of the state of the backups.

You can have your files restored by submitting a ticket to IT. To get the data restored from a previous backup, an IT manager must contact the third party who stores the data at an offsite location. The average data request takes around an hour to receive. Once received, they will replace the current data with the data that was backed up. The user can then verify to the IT manager that the backup is correct and then the help desk can close the ticket.

Once the backed-up data is no longer needed, the third party disposes of the backup data through a process called shredding. Shredding is where a device physically destroys the backup tape to a point where the data can never be recovered. Texas Roadhouse uses a third party to dispose data that is no longer needed. This process can be request by the information security managers at any time.

Texas Roadhouse is currently trying to move their data backup and recovery to the cloud. They have recently purchased a cloud service that they will use to store all their data on. This will probably be implemented sometime next year.

Using the cloud to backup and recover data will greatly improve Texas Roadhouse's information security. The cloud can transfer data within minutes, versus the hours it takes with backup tapes. The cloud encrypts the data and stores it on a remote server, which lowers the risk of loss that backup tapes have from events such as natural disasters [1]. This is a much faster process than requesting for the backup tape from the off-site third party. Also, since the cloud encrypts the data and is stored on a remote server there is a less probability of the data being stolen or lost. Since the third party relies on employees to retrieve and drive the backup data to Texas Roadhouse corporate, there is a higher probability that the employee could compromise the data or lose it.

The cloud minimizes the need for hardware, a trained staff, and hands on labor hours to backup data [1]. This makes the IT department more secure because the actual data backup tapes are not physically backed up in the data center where it can be vulnerable to people who have access to the data center. This can be a problem for physical security because sometimes technicians need to get into the data center to repair servers or switches. They could access the physical tapes and produce malicious activity. Therefore, Texas Roadhouse should move their data to the cloud, to eliminate their backup tapes and use the more efficient, and cheaper option.

**Training**

Texas Roadhouse provides certain training techniques to help insure employees are aware of the risks in the corporate office and in the restaurant. In the stores, they inform employees with what they should be doing and what they should not be doing while working in the restaurant. This includes, protecting all physical credit cards and the information on the cards. You should treat each credit card as sensitive information that should not be given out to anyone else. For example, make sure each credit card is returned to the correct guest. Employees should protect printed receipts and any paper that contains credit card information. If the receipt is not needed, shred it after processing.

One of the biggest risks to security is Point of Sale (POS) terminals. These terminals have direct access to the cardholder information. The need to check the POS terminals regularly for signs of tampering is a must. Things to check for are: new hardware plugged into the terminal and if the terminal is damaged from someone trying to open the terminal. Most importantly, informing employees of what they shouldn't be doing. This includes, not writing down information from a credit card, not using credit card data for any purpose other than the payment, and never leave credit cards unattended.

Some employees require more training and/or more advanced training than others. Support center staff must go through specialized training to be aware of unique information security vulnerabilities that they face as a department. The store managers should go through additional training to be aware of who can access what information. Only certain employees should be able to access the computers in the office and/or have limited access to the data on that computer.

The information security department at TR is responsible for creating, implementing, and maintaining the training program. All employees must participate in the training program and stay well informed on the policies provided by the training. These training programs are given to all new employees when they start at Texas Roadhouse. Also, all employees must attend information security training.

Improvements for training would be to create a policy requiring all employees (store and corporate office) to attend a refresher training program every 6 months. This training program would inform employees about information security and how to avoid hurting yourself or hurting the organization. Instead of using PowerPoint incorporate fun videos that employees won't follow asleep to. Who doesn't love a corny music video about how to create strong passwords. Another improvement would be to release an email newsletter every 2 weeks reminding employees about information security and how to avoid being the victim to a malicious attack. The more employees think about information security, the more secure your organization will be.

**Technical Security**

Texas Roadhouse sets up their network in a certain way so that they can comply with PCI DSS. In the restaurants, there is a single store switch that is used to connect the devices in the stores. Virtual local area networks (VLANs) are logically created off the VLAN to create a less flat network that improves security. Certain VLANs have certain machines connected to that specific network. For example, one of the VLANs has the printer, DVR, and a single computer used mainly for email and internet purposes. The most important VLAN in the restaurant is the cardholder data environment VLAN. This is the network that the POS terminals, back of house computer where all the cardholder data can be accessed, the wireless controller and access point that is used for the tablets to connect to the PCI network. To keep the network more secure the tablets do not communicate cardholder data. The only way to connect the cardholder data environment wirelessly is through certificate authentication which is what the tablets verify when connecting.

The switch/firewall is connected to two separate modems for redundancy purposes in case one of the connections go downs the packets can just jump over to the other modem connection. The first one is a DSL/cable modem, the second is a 3G//4G wireless carrier network. The DSL/cable modem connection is secured over the network by an IPsec VPN tunnel. The wireless carrier network is secured but not certain the exact way the connection is encrypted. The IPsec VPN tunnel and the wireless carrier network is then connected to a backbone router that is located at a third-party facility. The backbone router is a single router that can route both the wireless carrier network and the IPsec VPN tunnel. Texas Roadhouse uses their third-party facilities to house their own configured firewalls. From the firewalls at the third-party facility the cardholder data is sent to a bank payment processor where the cards are verified and the payment is processed. Some store management servers are connected to the firewalls at the third-party facility so they can remotely manage the stores. This is where another IPsec VPN tunnel comes into play. It travels from the firewalls at the third-party facility to the firewalls at the Texas Roadhouse corporate office to allow remote management of the restaurants.

To improve the network and technical security of the network, you could incorporate cloud based networking. Instead of using the traditional way of setting up WAN connections from the central network at the Texas Roadhouse corporate office to the restaurant networks. You use software defined wide area network (SD-WAN). What this method does is it virtualizes every network task used and delivers the task as a service. It is better than traditional WAN because it doesn't involve a mass grouping of single functioned machines connecting from different WAN links that causes complexity when managing. Also, the network management is logically centralized in software defined network controller software that sees the entire view of the network. The best part about it is the entire WAN appears to applications and policy management as a single logical switch [2]. This would decrease the cost of having a technician go to the restaurant because something went wrong with the WAN infrastructure at one of the restaurants.

This can improve security because you won’t have to rely on a manager at the restaurant to stay with the technician while he’s working on the network infrastructure. Who knows what he could get his hands on if he is left unattended. Also, it would increase the quickness and simplicity of setting up your WAN connections for every restaurant because all you do is set up a single Velocloud edge [2]. This is the only hardware needed to connect the restaurants to the corporate office.

After implementing the SD-WAN infrastructure you can provide security to your network by simply by using the orchestrator [2]. For example, creating VPN tunnels from corporate to the stores all with a simple click. Using a cloud based network while incorporating cloud based security would resolve issues Texas Roadhouse is having with two factor authentications. The current firewalls they are using cannot handle all the overhead from all the different users being processed through the firewall for two factor authentications. Using third party cloud based security you can easily incorporate two factor authentication services by connecting it to their cloud based firewalls through their orchestrator. All it involves is a couple clicks through the setup process [2].

Another improvement of technical security is using a password dictionary that would include restricted words. When creating a password for the back of house computer that has all the cardholder data on it, you couldn’t use those words. For example, currently you could create a password as “Password123” but with a password dictionary that has the word “password” restricted, you wouldn't be able to do that.

**Physical Security**

The Texas Roadhouse support center is in Louisville, KY. The building has a state of the art security system to secure all the offices. The system has a three day back up system in case of a power outage or a natural disaster. You must use a key card (smart card) to access the offices in the support center. These cards show the user's picture, name, department, and have lost and found instructions on the back.

To get a keycard, you have to make a request through the Support Services Department. If you are a new hire then you go through this request process during your orientation. The department manager/supervisor will fill out the request form with the new hires personal documentation. The new hire just has to go get his picture taken to complete the request.

Once this request is completed, it is sent to the Staffing Coordinator for them to manual enter the information into the computer. The system automatically sends out an email to certain departments on a need to know basis. A need to know basis is the principle of limiting users’ access privileges to the specific information requires to perform their assigned tasks [5]. Texas Roadhouse’s Risk Department is notified and can issue the keycard.

The amount of access you have within the corporate building is based on your job function. If an employee changes his job and/or his job function, then a request can be made to the Risk Department for them to change the employee's access. Whenever a keycard is lost or stolen, the employee is required to immediately notify the Risk Department via email. The Risk Department will make the employee a new keycard. The lost/stolen keycard is deactivated immediately, but will remain in the system in case someone tries to access the building using the card in the future. If someone does use this card in the future, the security guards will be notified and necessary action will be made.

If maintenance is needed on the network switches or servers then the IT department must call for a technician. When they get to the building they have to check in with the receptionist and then the receptionist contacts the manger. When walking through the building, there must be a manager with the technician always. You never know what the technician could be doing to the network while he is doing “maintenance”.

Both the corporate buildings and the Texas Roadhouse stores have cameras monitoring their equipment. They use closed-circuit television systems, that capture and record videos, to monitor the facility. These systems are important because they can record events that guards might miss. This video output is reviewed in real time by a security member [5].

Texas Roadhouse can work to improve their store’s physical security. We recommend they do this by putting a keypad on the door to the office which contains the stores back of house computer with cardholder data information. This will prevent unauthorized people or employees from walking in whenever they want. We also highly recommend the stores install alarms on their back doors if they are left open for too long. The back door is a way to enter the stores and is located right by the office. These doors are often propped open for convenience but this becomes a major security vulnerability. An intruder could easily walk in and go straight into the stores office. With an alarm that goes off if the back door is left propped open and a keypad on the office door, the physical security in the stores will be greatly improved.

**Works Cited**

Aldrich, Stephanie. "Tape vs. Cloud Backup." *Disaster Recovery and Business Continuity: EVS Corporation*. N.p., 3 Aug. 2015. Web. 28 June 2017. [1]

"SD-WAN vs.Traditional WAN." *www.velocloud.com*. Velocloud Networks, Inc., n.d. Web. 25 June 2017. [2]

Sr. Director, IT. “IT Cardholder Data Security Policy.” N.p., 22 May. 2017. [3]

Sr. Director, IT. “IT Wireless Security Policy.” N.p., 29 Apr. 2017. [4]

Whitman, Michael E., and Herbert J. Mattord. *Principles of Information Security*. 6th ed. U.S.A.: Cengage, 2017. Print. [5]