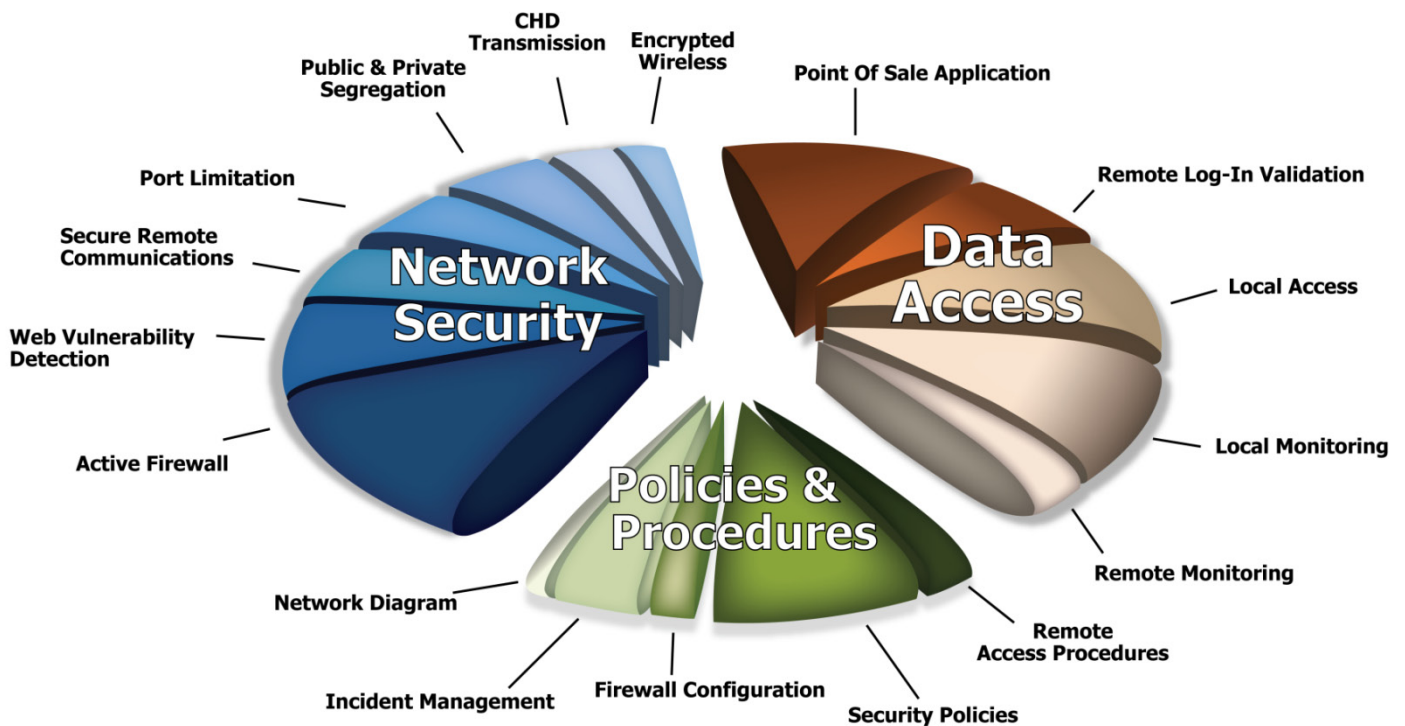


Case Study: Fast Food Franchise Security Breach (Multiple Locations)

by Bradley K. Cyprus, SSCP – Senior Security Architect, Vendor Safe Technologies

October 2008



Case Study: Fast Food Franchise Security Breach

Details

Period Summary for January – August of 2008 (Before Data Breach)

Industry	Hospitality – Fast Food
Sub-Class	Hamburgers
Hours of Operation	24 Hours / Day
Employees / Franchise	8-12
Annual Revenue (each)	\$1-2 Million
Credit Card Processing	High Speed Internet
Credit Card Integration	Fully Integrated with Point of Sale System
Wireless Network	Customer Internet Hotspot / Owner Access via Secure Wireless
IT Budget for Non-POS	Less than \$500 per Location

Profile

Case Study for a Fast Food Franchise

Company profile:

- The business is a franchisee of a national hamburger chain in the southern United States.
- As of August, 2008 they had 8 locations.
- Internal IT and resources and expenditures have been dedicated to maintaining their Point of Sale (POS) system. Little consideration was given for network maintenance (aside from supporting the POS installation), external security, or policy and procedures.
- Their POS system is a sophisticated application that allows for centralized management, financial and operational reporting as well as high speed Internet credit card processing.
- As a convenience, their customers were provided an Internet Hotspot that shared the high speed connection in use by the POS system.

Business Situation

This franchise relied upon the POS software reseller to be their de facto IT department. The reseller performed a standard installation of the POS software and associated hardware at each location. At some point, the environment was breached; malicious software, also known as malware, was installed on their network. Malware is designed to either to cause damage or steal information from a system, or both. As a result of the original configuration, at least 2 of the 8 locations had credit card data stolen from the systems electronically.

The malware was discovered at the locations where the security breaches occurred. Further analysis of the system uncovered that the shared Wi-Fi hotspots were not properly segregated, so direct access to the servers that processed credit cards was possible. It is likely that the Wi-Fi network played a role in the compromise of this customer's data by being a portal of entry for the discovered malware.

Case Study: Fast Food Franchise Security Breach

The franchise was notified by Visa U.S.A, Inc. and the U.S. Secret Service of the credit card theft, and now, a technical security audit will be required to validate the security and business practices at the compromised locations. The results of these audits and the extent of the theft will determine what type of fines and future requirements this business owner will face, assuming the franchises are permitted to continue to accept credit cards.

The franchise owner realized that the future of his business, in part, rested on how the security of the locations was improved. The franchise owner also became aware that the credit card industry had already created the guidelines to protect a merchant environment. The standard developed by six of the largest credit card brands is known as the Payment Card Industry Data Security Standard (PCI-DSS), and the theory behind it is that merchants who follow it will be less likely to be breached. The challenge was finding a way to quickly adopt the standard which has 226 requirements; many small businesses have found this challenging to implement – given their typical technical skill set. On the other hand, it is the only yardstick by which the major credit card brands measure the security compliance of a merchant. To become compliant, the franchise owner sought outside assistance to quickly achieve PCI-DSS compliance. He wanted a solution that provided unbeaten security that required minimal effort on his part, that had little to no impact on his business operations, and that fit a tight budget.

Technical Situation

The franchise owner had recently validated the security of his POS software to include the version number, so no upgrade was necessary to achieve PCI-DSS compliance. Each location has a computer network which included the terminals or workstations where orders are entered and the server which stored and processed credit cards. In addition, each location also has a wireless access point that was disabled once the vulnerability of the devices was discovered. Lastly, the customer relied on a Digital Video Recorder (DVR) system to record the activities of restaurants.

The primary goal of the franchise owner was to protect this network in such a way that would enable him to operate his business while still satisfying the requirements of PCI-DSS. To be successful, any additions to the restaurants had to be able to protect the systems against the threats posed by the Internet and malware. Customers would have to also be able to access the Internet wirelessly without compromising the integrity of the card holder data environment. Furthermore, a successful solution must include a remote access module so that the franchise owner, restaurant store managers and their POS reseller could access the locations from off-site computers in order to monitor DVR sessions, review operating reports in real time and provide ongoing technical support. While remote communication was critical to the customer, PCI-DSS has strict guidelines concerning the type of remote activity that is permissible and the logging that must accompany this type of communication.

Additionally, the franchise owner wanted to alleviate a technical issue associated with broadband failure. In the event any of the locations suffer an Internet outage, credit card authorizations cannot be processed in real time. The system stores the data and holds it until the Internet communication is restored. If a credit card, processed in this off-line mode, is denied, then the business cannot collect on the debt and potentially loses the money associated with the charge.

Case Study: Fast Food Franchise Security Breach

The Vendor Safe Solution

Turnkey security solution designed specifically for credit card merchants:

VST Global Security Mesh™ (Firewall with Integrated Services):

- **Best in Class Firewall** - Mitigates Internet based threats and protects the credit card environment. Both incoming and outgoing data is examined and managed before it is allowed to reach its final destination.
- **IP DataBlocker™** – Stop malware or individuals with access to the network from sending data to prohibited Internet locations from within the customer environment.
- **Rogue Device Manager™** – Detection and reaction in the event that an unauthorized computer system is physically added to a customer network. This will inform management of a potential issue by alerting them to the possibility that someone added a network device to their environment.
- **Real Time Monitoring** – 24 x 7 x 365 monitoring of traffic and error logs associated with communications and access. This allows the franchise owner to get a snapshot of the health of his network and to ask questions about potential issues.
- **Secure Remote Access Gateway** – Remote portal that allows secure access to system protected by the VST Security Mesh. For PCI-DSS, it includes two factor authentication.
- **Forced Configuration Manager™** – Automated access controller that validates the configuration of a remote system before allowing remote access. The franchise owner wanted validation on active anti-virus and active anti-spyware.
- **Automatic Broadband Failover** – Detects when the primary Internet connection fails and responds by initiating a redundant Internet connection. The redundant interface can be a second high speed Internet feed (cable modem) provided by the franchise owner, or as in this case, a dial-up modem connection provided as part of the managed service from Vendor Safe.

Hot Spot Plus™ (Managed Wireless with Integrated Firewall):

- **Managed Wireless Environment** – Provides wireless hotspot for patrons to use without jeopardizing the cardholder environment, clearly separating public vs. private network access.
- **Family Friendly Internet Browsing** – Content engine associated with the wireless environment so that prohibited websites are inaccessible from within the franchise owner's location. The franchise owner selected the categories of excluded sites to include porn, violence, and hate. The list of permissible sites is maintained by SurfControl, Inc. and updated automatically on a daily basis.

TrustVault™ Certificate (Mitigates the Cost Associated with a Breach)

- **\$50,000.00 Guarantee Against Data Breach and Credit Card Theft** – Vendor Safe offers protection against future fines and assessment in the event of a breach. While this does not improve security by itself, it gives the franchise owner the assurance that if our system is penetrated as was the case for his previous environment, we will help him with paying direct breach related expenses.

Case Study: Fast Food Franchise Security Breach

Benefits

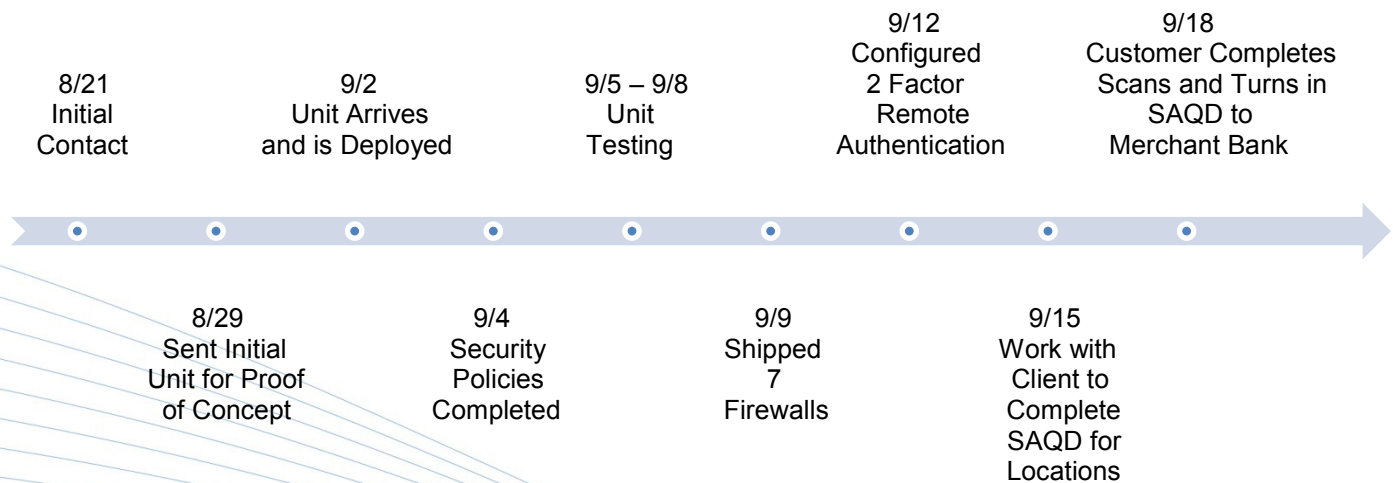
The franchise owner purchased the Vendor Safe solution and had it installed at every location in less than two weeks. By using this managed solution, the franchise owner reduced the required effort to become PCI-DSS compliant simply because this solution includes the necessary security and documentation that many small businesses find challenging. The bottom line is that the PCI-DSS evaluation was completed in less than 30 days after initial contact with Vendor Safe.

Now, the franchise owner has much greater security at every location that includes monitoring and protected remote access. Upon termination, the remote access privileges of an employee can be revoked immediately from the centrally managed infrastructure. This ensures that a disgruntled worker is unable to cause havoc or threaten the card holder environment from the Internet. In addition, the franchise owner has the wireless access they need for both internal use and public convenience, and a partner willing to guarantee their solution for \$50,000.00 at each location.

Since the system was deployed, several unauthorized remote access attempts have been blocked and internal threats have been thwarted. The system reports errors in real time, and the Vendor Safe staff monitors the traffic to help prevent further credit card issues. When broadband failures occur, the monitoring center records the outage while automatically restoring Internet communication using a dial-up connection. Vendor Safe then works with the Internet provider of the customer to remedy the communication issues. The Vendor Safe solution solved both the security and business process issues experienced by this customer.

Deployment Time Line

From First Contact to PCI-DSS Compliance



Make a secure move, call Vendor Safe at 713-929-0200
7324 Southwest Freeway, Suite 1700
Houston, TX 77074
vendorsafe.com
info@vendorsafe.com