CASE STUDY: ARS

Situation

ARS®/Rescue Rooter® are headquartered in Memphis Tennessee and provide cooling, heating, and plumbing services with a knowledgeable team of trained specialists.

ARS's Regional Call Centers take calls for 70 businesses across the United States. Their call center agents generate a work order and problem details and then processes them to local dispatchers. The dispatchers schedule the technicians to the customer home or business sites. After the work is completed, the technician takes payment either by check or credit card. The technician calls into dispatcher with payment detail and to close the work order.

ARS Dispatchers use the Chase Paymentech Virtual Terminal to process the payments real time while the technician is at the customer site or home. This gives the technician the flexibility to accept multiple types of payment and bill according to the work completed. It also affords ARS the benefit of receiving real time payments instead of waiting lengthy periods for the payment of invoices, and reduces the need for collections staff and costly paper trails. Also from time to time the accounting personnel use the Paymentech Terminal for reconciliation. ARS do not use VoIP and do not record calls internally.

ARS started with an initial 350 users in 56 locations with an expected growth of several times this.

Business Case

The use of an outsourced payment solution accessed via remote browser or 'Virtual Terminal' sessions creates a requirement for a number of additional compliance controls. Per the PCI DSS 3.1 requirements, anything that 'stores processes or transmits' cardholder data is 'in scope' for PCI compliance. That means that all workstations, local area networks, wireless networks, applications or systems within the cardholder data flow need to be protected by a number of controls. While the virtual terminals reduce the requirement for housing payment applications on site, they provide nothing at the merchant end to isolate the session or protect the workstation and therefore at least 10 out of the 12 PCI requirements still apply. In the case of ARS, they have a large number of agents, distributed across multiple sites and needed to attain compliance fast without significant changes to existing processes that would affect their customers. ARS management was not willing or able to reduce the number of agents or sites with the ability to take payments and thereby reduce their high level of customer service.

The main objective of the Senior Director of IT Operations was to

- achieve PCI DSS compliance
- reduce scope as much as possible
- expand user base and numbers cost effectively and efficiently
- Permanently remove company network segments from scope of future assessments
- Reduce complexity of the infrastructure and data flow for PCI
- Retain the same payment gateway agnostic so that provider could be changed at any time without problems or large financial outlay
- Further reduce scope and risk by including additional features at some future date such as eliminating call recordings and agents from scope

Possible Solutions

ARS had as options a number of possible solutions:

- **Dual Workstations**
  Prohibitive due to costs, space and the lack of administrative control to ensure both required controls were implemented but also managed and testable. This solution is not user friendly.
- **Hypervisor**
  As above, without full administrative capabilities over requirements 2, 5, 6 10 and 11 it hard to implement, manage and test appropriately and required a lot of additional logging.
- **Homemade USB key**
  Device management, network segregation, tampering, removing in addition to the standard admin workload plus patching, logging, etc. made this a solution more suited to at home or Internet Café browsing vs a locked down compliance environment.
- **Commercial 'VPN Device'**
  The devices are secure, portable, reasonably priced and enabled central configuration, device locking, and session clearing. However, a central VPN device is required at additional costs, there are still issues with device distribution (physical) and management; initial credentials could be key logged and there was no ability to segregate networks in the absence of the vpn device.
- **A Commercial Secure Virtual Workspace**
  Similar to a usb device but software, not hardware based, however, OS/Browser support and updates are a concern and requirements/needs may not be met in a timely manner. Internal management is still required unless it is fully outsourced in a hosted environment.

Their IT staff had been evaluating various options for segregating these workstations and had found no financially viable solution to eliminate the need for controls on these workstations and attached networks.

Solution

DataDivider Virtual Keypad (VK) is a QSA approved compensating control for Virtual Terminals so that the workstation, keyboard and screen are isolated so that there is no chance to log keystrokes or capture screen shots. DataDivider completely de-scopes both the local network and desktop from PCI scope by ensuring the cardholder data never crosses that network and uses a number of different controls to protect against malware, viruses, data leakage and any type of frame grabbers to protect the desktop. Each agent has an individual profile, locking down all activities to only those that they are authorized to perform and all policies are protected within a PCI compliant environment. It is secure, PCI approved and hosted within a fully managed level 1 PCI compliant datacenter. DataDivider VK can be implemented within 24 hours with no disruption to merchant services.

- DataDivider VK removes workstations from scope via compensating control (annual validation required)
- DataDivider VK removes your local wired or wireless network from scope
- The separate, segregated/protected browser operating in its own memory
- Security software validates compliance/safety of workstation (patches, A/V, etc.) before opening this session and deletes the data at the end of each session
- End user logs into a desktop session over a secure encrypted link within a secure browser session to a URL at DataDivider instead of directly to the payment gateway
- PANs are not directly input by or processed through your actual workstations All screen copy/paste and other interactions between normal host session and VK session are blocked
- Payment card fields are blocked from normal keyboard input and masked (customizable)
- A virtual keypad is used to input the PAN and other sensitive
- It can be configured to send any authorizations back to the customer along with a tokenized version of the card number
- No changes required on workstation side and no management required by customer
- If you host your application internally or externally, no changes need occur other than connecting to a different URL
- Any payment gateway, web based application and token can be used

Outcome

ARS selected DataDivider VK and have eliminated the need to implement any further controls on their agent workstations for connecting to Chase Paymentech. Their local networks are also out of scope for this connectivity. They have since continued to expand their number of agents to over 850 and 63 sites. Each user can be added and removed independently in any location without any other changes other than whitelisting of new sites. While paper records and offline data still remain, future projects would allow ARS to securely upload and store any sensitive data within DataDivider or PAN could electronically be replaced by a meaningless token to completely eliminate the requirement for further electronic or paper storage locally.

“The DataDivider Virtual Keypad helped us secure our agent environment without impacting the high level of service that our customers expect. The DataDivider Solution was easy to implement and integrate with our existing software with minimal staff training and no costly infrastructure changes. The assumption that telephone payments would die out just does not apply to our industry. In fact we are increasing our call centers in both number and size to offer a more personalized service to our customers and to generate higher average sales.’

ARS were able to reduce significantly their PCI DSS scope and achieve significant cost savings, the extent of their assessment and the number of controls that they need to manage and also have the scope to reduce this even further with minimal expense or process changes

DataDivider are currently working with several processors to provide for their customers to take their systems out of scope and offer CRM, ERP and full voice solutions as well as Virtual Keypad with messaging and fax.