datadivider

CASE STUDY: Higher Education – Principia

Situation

Principia College (commonly referred to as Principia or Prin) is a private liberal arts college in Elsah, Illinois, United States. A four-year coeducational institution, the college was founded in 1912 by Mary Kimball Morgan, and its stated purpose is "to serve the Cause of Christian Science." The campus is located on rural total of 2,500 acres (10 km2) acres in the Metro East region of Southern Illinois, thirty miles north of St. Louis. Principia is a Tier 4 merchant with 5 merchant ID's at their main campus. They have a hosted virtual terminal solution with staff of 10 processing transactions via their virtual terminal.

Business Case

The use of an either in-house or 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, 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 Principia, they have a small number of agents, distributed across campus and therefore did not feel that they wanted to budget for and manage a large number of controls.

The main objective of the Head of Compliance was to

- achieve compliance
- reduce scope as much as possible.
- Permanently remove network segments from scope of future assessments
- Reduce complexity
- Remain payment gateway agnostic so that provider could be changed at any time without problems or large financial outlay

Possible Solutions

Principia had as options 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**

This requires mixing Virtual Machines of different trust levels and mixed-mode environments. 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.

The University 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 Protected Zone (PZ) 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 PZ can be implemented within 24 hours with no disruption to merchant services.

- DataDivider PZ removes workstations from scope via compensating control (annual validation required)
- DataDivider PZ 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 DataDivider PZ 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

Principia selected DataDivider PZ and have eliminated the need to implement any further controls on their agent workstations. Their local networks are also out of scope. DataDivider are currently working with several SaaS providers of campus management solutions provide a way for their customers to take their systems out of scope and offer CRM, ERP and full voice solutions as well as DataDivider PZ with messaging and fax.