

DATA SECURITY Bulletin



6-7-2010

As many of you heard at Partner Summit in January, Radiant is committing significant resources and efforts to helping our customers secure consumer data. We want to ensure customers understand their responsibility related to data security and liability per Payment Card Industry Data Security Standards (PCI-DSS) and card brand mandates. We will be promoting awareness by educating our customers on the following areas on which they need to focus to enhance the security of their business:

- **1.** Implement secure remote access practices
- **2.** Implement adequate password controls
- **3.** Regularly perform procedures to securely remove any sensitive data no longer needed and securely delete any unallocated space
- **4.** Install a hardware firewall
- **5.** Install anti-malware programs
- **6.** Ensure you are running version 7.5.12 CounterPoint or newer, or version 8.3.3 CounterPoint SQL or newer and configure your system to do the following:
 - -Enforce strong passwords for all users
 - -Store full credit card numbers only if you have a critical business need for the information
 - -Display the full credit card number in ticket history only to employees with a critical business need for the information
- **7.** Ensure your operating system is up-to-date with security patches
- **8.** Prove compliance at specific points in time (SAQ/network scans)

- **9.** Implement operational security processes
- **10.** Consistently monitor your security infrastructure and procedures

As their service provider, you are in a unique position related to data security at your customers' sites. We want to make sure you are aware of recommended security practices when implementing, upgrading, or supporting your customers. In the coming months, we will be providing you with best practices to help you understand the PCI-DSS requirements related to each of the 10 areas of security focus identified above.

What Can You Expect From Radiant Systems

- Ongoing security bulletins and webinars providing details on the PCI-DSS requirements and best practices related to each of the 10 areas of security focus identified above. **Our next data security communication will be on Monday April 19th and will highlight implementing secure remote access practices.**
- A public website to educate existing customers and prospects across the retail industry with topics such as:
 - **PCI Compliance 101** - overview of the 12 PCI DSS requirements and what that means to retailers
 - **Data Security Milestones** - timeline of key dates regarding data security and compliance
 - **What you can do today** - key areas of concentration for protecting a site from risk (network configuration, remote access configuration, Windows/OS configuration, user management, POS configuration, auditing)
 - **Life Cycle of a Security Breach** - what happens to a retail merchant if they do get breached and the costs associated with this
- An enhanced data security section on counterpointpos.com including all the information on the public website with additional information related to security and compliance related specifically to CounterPoint.
- Posting of each of these data security bulletins on mySARA..
- Central contact point for questions related to PCI compliance and data security: datasecurity@radiantsystems.com.