

# DATA SECURITY Bulletin



## Monthly Data Security Webinar

These monthly webinars will be an opportunity for Radiant Retail Partners to ask questions about the information contained in our data security bulletins. Our first webinar is scheduled for **Wednesday May 5 from 3:00-4:00 PM EST. [Register Today!](#)**

### **Data Security Q&A Webinar:**

- Ask your questions about the most recent Data Security Newsletter
- Gain insight from Radiant about commonly asked questions
- Get more information and/or updates from Radiant Experts about Data Security

## Security Practice-What is Secure File Removal?

Many people do not realize that simply deleting a file does not mean it cannot be recovered. File deletion is different than secure file removal. When deleted, a file moves to the Recycle Bin but the link still points to the file retained on the hard drive. The space previously occupied in the hard drive is now freed as unallocated space. The retained file is only overwritten when the drive space is needed. On larger drives it will take years for this to happen. Secure file removal is a secure method of ensuring that data is irrecoverably deleted and helps you avoid potential exposure associated with the support of sensitive data such as track data, account numbers, etc.

An example of the exposure that can be associated with not securely removing files is highlighted in a 2003 research study from MIT. Two students purchased 158 used disk drives from readily available sources for used computer hardware. Of those 158;

- 81% were functional
- 60% of the disks were formatted
- 45% of the disks contained no files, yet data was still retrieved from them
- 18% had little or no attempt to erase information
- Less than 8% were properly sanitized
- One came from an ATM and contained a year's worth of transactions

From those drives, over 5000 credit card numbers, personal and corporate financial records and medical records were found.

### **When should I run a secure file removal process?**

Secure file removal utilities can be used to wipe a file, folder contents or entire hard drive. If you are supporting sensitive data, you should perform a secure file removal on your hard drive:

- Sensitive data includes any data surrounding a credit card: account number, card verification number, PIN, or especially track data. It is also a good idea to treat personnel information such as Social Security numbers, etc as sensitive.
- Any time sensitive data is written and no longer needed for business purposes

- Sensitive data includes any data surrounding a credit card: account number, card verification number, PIN, or especially track data. It is also a good idea to treat personnel information such as Social Security numbers, etc as sensitive.
- After any update of CounterPoint or other payment application
  - Updates include major release changes as well as minor service pack installations
- During hardware return to service. Even if hardware is ghosted, this does not necessarily mean it was securely wiped. (Radiant uses secure file removal procedures on hardware returned to Shiloh office.)

In addition, when you have completed work on log files or transaction files containing sensitive data, you should place them in a single repository. This repository should be wiped frequently, at least once weekly. Some file removal utilities allow you to set this up as a recurring task, but it can also be done manually.

**NOTE:** Depending on drive size, this process will take more than a few hours and should be performed during a scheduled period of prolonged down time

### **What are some tools I can use?**

Data can be securely removed using a number of different utilities. Radiant currently uses the following secure file removal tools:

- **sDelete v1.51** - a freeware command line tool used for secure data removal and wiping of hard drive space. You can download this tool at <http://technet.microsoft.com/en-us/sysinternals/bb897443.aspx>
- **Eraser v5.8** - An advanced freeware security tool which allows complete removal of data from disk drives by overwriting it several times with carefully selected patterns. You can download this utility at <http://eraser.heidi.ie>

If you have questions or concerns about using a secure file removal utility, first contact the technical support function for that utility. If you have additional questions related to secure file removal, email us at [datasecurity@radiantsystems.com](mailto:datasecurity@radiantsystems.com).

These guidelines help secure your business today. Please note, however, that there are more requirements than outlined here to be PCI compliant. More information about PCI requirements may be found at [www.pcisecuritystandards.org](http://www.pcisecuritystandards.org).