

An important challenge for today's bookstores: Keep Your Data Safe and Stay PCI Compliant

Twenty years ago, bookstore managers were more worried about thieves making off with the products on their shelves than with stealing their data. Times have changed. Today, IT security has become one of the biggest concerns for bookstores. Payment Card Industry (PCI) Data Security Standard compliance is a key responsibility for bookstore operations.

"There's a lot at risk for stores that don't take care of their data," says Kevin Wright, Vice President, technology, Nebraska Book Company. "No one wants to be known as the store that had credit card or identify theft. Your reputation is at stake, both with your customers and within the industry."

Statistics show it costs 20 times more to deal with a data security breach than it does to put safety measures in place beforehand. With that in mind, Wright offers strategies for creating a solid security plan:

Use the Five Best Practices for IT Security

- 1. Take Stock.** Know what information you have. Inventory your files and computers. Know where it's collected, where it's held, how it's used and how long you'll need it. Be aware of industry regulations or laws that may impact your business. Rate the risk associated with any sensitive data.
- 2. Scale Down.** Be lean. Keep only the sensitive data you need for your business, and only as long as you need it. Don't use Social Security numbers or other sensitive data as account numbers. Minimize the number of people that have access to this information and the number of places the data is kept.
- 3. Lock It.** Ensure physical security by installing locks and controlling access. Stay up to date with firewalls, intrusion detection systems, antivirus software, patches and encryption. Document security policies, conduct background checks and maintain a culture of security; that includes your service providers and contractors.
- 4. Pitch It.** Put in place reasonable disposal practices; shred physical copies of documents. Use special "wipe" programs to delete electronic copies. Be sure employees working from home or on other systems follow the same procedures. If you use background checks, you may be subject to the FTC's Disposal Rule – make sure you are up to date with that process, too.
- 5. Plan Ahead.** Have a plan for how to respond to security incidents. Designate a senior staff member to coordinate and implement the plan. If a bookstore computer is compromised, disconnect it from the network. Investigate breaches immediately and report them promptly.

Make PCI Compliance a Priority

Payment Card Industry (PCI) Data Security Standard compliance isn't just about selecting the proper software to keep credit card data safe, explains Wright.

PCI compliance is a critical part of a retailer's operations. Compliance standards include six topic areas and 12 high-level requirements. Merchants are divided into four levels, but the requirements are the same for all levels-only the auditing and deadlines vary. Every retailer must perform quarterly network scans to ensure their systems are secure.

Here are some important steps to keep your bookstore PCI compliant:

- **Partner with a Qualified Security Assessor**, an individual or company that Visa and MasterCard have approved or certified. Find a list in the Resources section at www.pcisecuritystandards.org

- **Use a validated payment application**. It may not be required today, but chances are it will be in the future. For example, Wright explains, the payment application used by the Nebraska Book Company retail management software has been validated and appears on Visa's web site.

- **Scale down**. Instead of making every computer on your campus PCI compliant, keep credit card data on one portion of the network and protect it with a firewall. It's less expensive, safer and easier to do.

Once these steps are built into the daily operations for your bookstore, the safety of the data will immediately improve. Your customers will appreciate your concerns for their safety!