Current Technology Trends as it Relates to the Independent College Retailer

Nate Rempe has been with Nebraska Book Company since 2005, rising from Director of Internet Strategy to Vice President of Internet Services to Senior Vice President and Chief Technology Officer. A multiple patent holder and member of the executive faculty at Creighton University, Rempe built NBC's technological competencies to include Web Development, Desktop Development, Mobile Development, Mainframe and Legacy Development, Enterprise Development, Integration and Architecture, IT Operations and Infrastructure, Data Warehousing, Software Training and Documentation, Software Technical Support, Software/Hardware Quality Assurance, IT Project Management, and Business Systems Analysis. These are all used in NBC's pursuit of the success of independent college retailers.

It used to be that the local store was a social hub as much as a place of commerce. Customers knew the owner, the employees were neighbors and used their patrons' first names. It still is that way in many cases, but with the rise of online shopping and purchases, merchants have had to split their time and attention.

Suddenly, human interaction was not the only focus for doing business, and both fronts suffered, from the decreased customer service priority and the lack of expertise with technology and ecommerce. However with the right partner, both can be strong contributors to a thriving independent college bookstore.

Retail technology is very important for independent college retailers, but it is not their most important responsibility. We at Nebraska Book Company are transforming our business to one that offers the products and the services to manage those products on our customers' behalf. This way, stores can focus on what matters most: delivering best-in-class service, and building relationships with students, faculty, and the community. The viability of the college retail store absolutely depends on being able to focus on those things and that's why providers that offer Managed Services - again, not just the tools, but also the services to manage them - has to be where bookstores start looking for help.

Speaking of help, of all of a retailer's technological concerns, the security of sensitive customer information is arguably the most crucial and the most challenging. The protection of customer financial information, whether through online or in-store transactions, is necessary for repeat business; if customers can't trust a retailer to safeguard their credit card data, they won't be back, and we all know the press is unforgiving when it comes to lacking data security. Complying with the most recent Payment Card Industry Data Security Standard (PCI-DSS) is the best way to ensure customers are protected.

If retailers don't pay attention to data security, they take on a lot of risk. The good news is that this is an area in which technology can really take much of the pain away. The key to PCI compliance is to simply not have any credit card information stored on a retailer's system.

Reducing the scope of PCI compliance translates to less work, less risk and less cost, and the impact to the retailer of lock-tight card data security is that fraud is much less likely to happen online and at the point of sale. NBC provides that worry-free experience with point-of-sale and ecommerce coverage.

NBC's point-of-sale product, PRISM 360, in partnership with payment gateway provider Shift4 Corporation, provides a cutting-edge solution called point-to-point encryption (P2Pe). P2Pe is a hardware-based encryption that happens at the PINpad and communicates directly with the merchant gateway so that credit cards never exist and never flow anywhere on the network. They are never stored in the back office, and as a result, stores don't have any credit card data anywhere on campus.

At University of San Diego (USD), we're rolling out PRISM 360 campus-wide, making all POS transactions immediately PCI compliant with very low scope because there is no credit card information anywhere on their campus system. Every transaction will utilize point-to-point encryption. USD is a good use case; our system was certified on campus by an entity called Campus Guard, a third party organization that qualifies systems as being secure and compliant.

Recently, retailers faced a deadline for their POS system to be certified to accept payment from cards with EMV technology. Designed to heighten physical card security, EMV cards contain a chip that PINpads must read before the card holder signs to complete the transaction. Since these cards are inserted into a reader, not swiped, the PINpad must accommodate them. Retailers who did not meet the July 15 deadline for EMV certification take on additional risk for fraud.

PRISM 360 in partnership with Shift4 Corporation also delivers out-of-the-box EMV-ready PINpad technology so schools can have not only PCI compliance with P2Pe but they can also be EMV-certified in campus convenience stores, dining, concessions--anywhere a point-of-sale transaction is happening.

I caution schools and retailers, however; having EMV PINpads is only one piece of the security puzzle. In a recent article, Greg Buzek, president of retail research and advisory firm IHL Group, said:

EMV only resolves one piece of security, and it's the least concerning piece. The biggest concern for retailers is a data breach, and EMV doesn't really help in any way regarding a data breach. EMV also does nothing to help keep online transactions secure. Retailers that are not putting additional security measures into place to protect their online transactions are going to find themselves in situations where a certain amount of card fraud at the store level will increase greatly online."

According to the 2014 LexisNexis® True Cost of Fraud Study, in 2014, 51% of fraud happened online. That's up from 42% the prior year. Many retailers focus on having "offline" compliance in their physical environment, but the truth is that's quickly becoming most unlikely place they're going to see fraud. It's more likely they see it on the web, and that's the most difficult place to protect.

From an ecommerce perspective, NBC, its data center, and its ecommerce solution is Level 1 PCI Data Security Standard Certified, meaning schools and retailers using our Managed Services enjoy an ecommerce site that provides them the highest level of online information security available.

With our solution, independent college retailers can have next to no concerns about data security. We've got a trusted, secure area in our data center where we store sensitive data and the controls and technology protecting that data were certified by the PCI Security Standards Council.

The majority of people don't realize that in most cases fraud isn't discovered by a company seeing it happen on its systems; it's identified by customers notifying their credit card companies of suspicious purchases. Most often it's when multiple instances are reported, and when fraud departments look back to see where those cards were used many times they see exactly where the breach happened because 20 people reporting fraud all shopped at the same location.

That's why it's important to always be on top of card data security, because oftentimes you don't know you've had a breach. And you'd be surprised at how many of the retail technology and ecommerce providers today are not PCI certified.

For example, you can use a data center that is a PCI-DSS Level 1 Certified but that doesn't mean your application is certified. Whether it's an honest misunderstanding on the part of the provider or lack of diligence on the part of the customer, it's important to not only make sure the data center (the physical environment itself) is secure, but also that the application, the servers, and the network running the system are certified.

The bottom line is, NBC's solution is more secure because it comprises the six necessary parts:

1) The POS (PRISM360), ERP (WinPRISM), and ecommerce (WebPRISM) systems all support P2Pe (or point-to-point encryption).

2) The POS (PRISM360) and ERP (WinPRISM) systems are PA-DSS (Payment Application Data Security Standard) validated.

3) The ecommerce (WebPRISM) system is Level 1 PCI-DSS certified.

4) The ecommerce (WebPRISM) system is hosted in a data center that is Level 1 PCI-DSS certified.

5) The POS (PRISM360) and ERP (WinPRISM) system support EMV (in partnership with Shift4 Corporation).

6) NBC employs two PCI-ISAs (PCI Internal Security Auditors) and provides on-site PCI-DSS consulting services to help identify areas of risk and propose solutions for mitigating that risk.

As far as I know, no one else in the industry offers this level of comprehensiveness in security and compliance. Knowing that fraud risk and liability concern is being managed by a trusted partner frees college retailers to concentrate on the human side of their business: the customer and the community.