Data Security: Reaching Beyond Compliance

LP Magazine interview with Paul Murray

Paul Murray, a founder of Wontok, Inc., sets the strategy and direction of Wontok's solutions development as well as managing operations out of North America. With more than fifteen years' experience in high tech and telecommunications, Murray combines his technical background with project management and team building. His previous role was CTO of Protel Communications, a company he also cofounded, which was acquired by M2 Telecommunications in 2006.

EDITOR'S NOTE: Building on common ground improves comprehension and enhances professional development. One way to accomplish this is by asking the experts—those with exceptional ability and expertise to explain concepts, products, and functions in terms that can be easily understood and applied in everyday situations.

Data security is a critical subject that demands the attention of every LP practitioner, and bridging the gap between LP and IT remains essential to our future success. LP Magazine *recently sat down with Paul Murray, senior vice president of product management for Wontok, Inc. to help bring insight into building these relationships. Wontok's industry expertise is bringing value-added data security services to businesses across the U.S., Europe, and APAC.*

What are the biggest hurdles that retailers face when building an effective communications bridge between LP and IT?

Information exchange and collaboration is the key. Loss prevention and IT need to form a partnership with a common language that embraces the financial as well as the technical, especially considering how that pertains to data security. Technology alone won't bridge the gap. Some of the biggest challenges in business are changes to the culture, and the fundamental challenge here is cultural.

We can't allow either of these departments to operate in a silo. Some changes will require IT and LP to work more closely together at a compliance level, which helps build a common language. Working together and having like goals is a natural catalyst for creating a more cohesive working relationship. If the business can implement a smooth and accommodating change in the way these departments work together, the results will follow.

How can LP educate or share intelligence with IT to help keep the business protected?

LP departments typically have excellent intelligence on the human factors that impact the business. Contractors, suppliers, and even staff turnover are all in view of and understood by LP. By bringing IT into the fold, IT will be better armed with potential breach vectors beyond those that originate from the Internet, but are just as dangerous. For example, if there is a process in place for outside vendors gaining access to systems for maintenance, then both LP and IT should be involved in the process. Not only will this approach help to automate the process, but the entire organization will be more alert to any additional data breach vectors that can then be addressed.

What are some ways that IT can educate or share intelligence with LP to improve network protection?

This information exchange should start out simple and avoid becoming overcomplicated. Data security can be a complex topic, but it's critical to remember that a sound understanding does not require a deeply technical comprehension. By gaining clear insight on the basics of sensitive data, how it moves around the network, and how it is stored, LP staff will develop awareness in their day to day. Over time, data will simply become another valuable asset that needs to be protected, similar to merchandise, profits, and brand.

How will the new and interactive technology being introduced into the consumer experience influence the need for LP and IT to work together?

With technology making its way into all industry sectors, there are great benefits to collaboration between LP and IT. Take customer Wi-Fi for example. There are areas of a retail premises that are clearly off limits to customers, such as offices and stock areas. But when we offer customers access to free Wi-Fi while they shop or dine, have we given this the same degree of thought? If your Wi-Fi is on the same network segment as your back office servers, you might as well have customers passing freely through this area. Collaboration on decisions like this not only limits mistakes, but increases awareness and merges responsibility and expertise.

Cooperative efforts should also extend to staff training. By enhancing sales training to include more technical information on the equipment being used and how it can be used against us, we may be more apt at thwarting criminal incidents that may have otherwise gone unnoticed.

Why is it so critical for retailers to look beyond compliance to protect the business?

Simply stated, being compliant is not the same as being secure. The retailers recently breached were compliant. We need to go above and beyond these regulatory recommendations, work together, and take the necessary steps to be as secure as we can be if we don't wish to become the next victim. ■