Information Sharing

An Interview with Tom Litchford,
Vice President-Retail Technology, National Retail Federation (NRF)

EDITORS' NOTE *Prior to assuming his current position in July 2012, Tom Litchford held key Microsoft positions in industry sales, marketing, and channel management. Before joining Microsoft in 1998, he was Director of Business Impact Modeling for NCR's Retail Solutions Group. Litchford was instrumental in driving the development of the OLE for Retail POS (OPOS) application program interface (API) – now a de facto industry standard for point-of-sale application-to-peripheral connectivity. Working with organizations such as ARTS and the North American Association of Feed Equipment Manufacturers (NAFEM), he has also been influential in establishing XML messaging standards in the retail and foodservices sectors. Litchford holds a bachelor of applied science degree in computer systems from Florida Atlantic University.*

Tom Litchford

ORGANIZATION BRIEF *NRF (nrf.com) is the world's largest retail trade association, representing discount and department stores, home goods and specialty stores, main street merchants, grocers, wholesalers, chain restaurants, and Internet retailers from the United States and more than 45 countries. NRF's This is Retail campaign highlights the industry's opportunities for life-long careers, how retailers strengthen communities, and the critical role retail plays in driving innovation.*

What are the issues that the CISOs you work with are concerned about and what needs to be done to continue to address these challenges?

The cyber crime issue is not just a retail industry problem; it is a business risk problem facing all industries. The government is fighting it, too; it is a cyber war that we're fighting.

In retail, we're mostly dealing with cyber criminals as opposed to nation states. These bad actors are looking for data they can easily monetize, and unfortunately they've found a gold mine with credit card data over the past few years.

Under the direction of the CIO Council, we developed an IT Security Council with the number-one objective being to foster a community focused on information sharing. If we can create better situational awareness of what is going on relative to cybersecurity, not just within our own organizations but within the industry and beyond, we feel we can help our members better defend themselves.

Specific to information sharing, we have focused on a few things. NRF runs a threat alert system that pushes out around 12 to 15 alerts per day. We get these alerts from several sources, including the Department of Homeland Security where we have access to US-CERT and the NCCIC and their cyber information and intelligence.

We have a strong relationship with the United States Secret Service as well as the FBI, and we have relationships with the FS-ISAC, which is the financial services industry's Information Sharing and Analysis Center (ISAC). Considering the cyber criminals right now are most interested in stealing credit card data from retailers, having a good relationship with the financial industry is pretty important.

Speaking of credit card data, what are retailers doing to protect it?

Excellent question considering the misconception that the EMV (or chip and signature) cards mandated by the financial industry are the panacea. This is an area where we disagree. EMV does nothing to protect credit card data, especially without a PIN like the rest of the world uses. Last month's Black Hat event also demonstrated that EMV cards are easily hackable for making counterfeit magstripe cards. Knowing this, retailers are busy implementing P2P encryption and tokenization – security solutions that are much better at eliminating the value of any stolen data.

The conversation today around cyber seems to be more about reacting to the issue as opposed to prevention. Does more need to be done to address prevention?

In the past, most of the focus has been on perimeter defense. While we're not saying that perimeter defense isn't still important, we're dealing with some fairly sophisticated bad actors and they're likely to eventually find a way in. This means we need to also focus on breach detection and mitigation. This involves a broader cyber security program or strategy than we might have had in the past. Also, we see most retailers implementing a strong incident response plan, and getting more sensitive to data classification and the types of data they choose to retain.

Is the proper dialogue taking place to enhance the recognition of the challenges around classified information and broadening the need to share information?

The question is spot-on in noting that cybersecurity information sharing is one of the most important things we can be doing to better defend against cyberattacks. To do that takes trust. Bill Nelson of the Financial Services ISAC told me it took their organization 10 years to build trust and to start seeing financial organizations sharing cyber intelligence among themselves. I certainly hope it doesn't take retail that long but it is a bridge that we need to get across.

NRF is working hard to help establish that trust and facilitate rich information sharing. First, it's hard to trust someone that you don't know. This means we need to bring these groups together throughout the year so they can start building a camaraderie and put aside the idea that we're competitors. There is nothing competitive about cyber defense.

Additionally, it requires working with the general counsels and convincing them that there is a huge benefit to allowing this sharing to go on. The counsels are very concerned around privacy and liability, which is one of the reasons NRF strongly backed CISA (Cybersecurity Information Sharing Act) that was passed in December of 2015, which provides liability protection and privacy guards when one is sharing cyber information.

Is it hard to be optimistic when it comes to how big these problems are and can they really be addressed effectively?

We certainly celebrate our successes when we hear these groups or individuals are getting busted, but I hate the pessimist view that we have to get it right all the time while the bad guys only have to get it right once. I like the metaphor of the Cyber Kill Chain.

The kill chain was originally developed by the military during the Gulf War in response to IEDs being deployed on the side of roads to take out convoys. The theory behind this, which has now been applied to cyber (by Lockheed Martin), is that if we look at the process that these bad actors have to go through to be successful, there's a chain of events that are linked together. We only have to break the link in one place to stop a successful attack. It's referred to as "staying left of boom." As long as we're getting the intelligence and sharing the information we need to in order to figure out where we can break the link at a certain point in their attack plan, whether that's during reconnaissance, compromise, exploitation, establishing command and control, or exfiltration of data, then they're not going to be successful.

I like to take the optimistic view. They're sophisticated and smart, but we are too. ●