Digitizing the Customer Experience for Restaurants: A Recipe for Success

By Aaron Branson, Cybersecurity Market Strategist, Netsurion

The restaurant industry is undergoing a dramatic shift, focusing on a digital transformation of the customer experience (CX). Restaurants, like retail, are scrambling for more digital experiences to attract new customers and for personalized engagement to keep the customers they gain.

CX IS A HOT DISH

CX initiatives can help make the restaurant experience more engaging and extend the interaction with customers beyond the brick and mortar. Offsite CX initiatives include online ordering, loyalty programs, digital menus, and feedback and personalization mechanisms. On-site there's mobile payment, order kiosks, and tabletop tablets. And that's all just for starters.

So, what makes a restaurant customer experience a "better" customer experience? And what are customers looking for in choosing a restaurant or in coming back time and again? The following figures are taken from a 2016 research study conducted by Deloitte:[1]

- **Online ordering:** 40% of customers prefer to **order online**, and when they do, **spend increases** 26% in quick serve restaurants (QSRs) and 13% in casual / fast-casual.
- **Loyalty programs:** 87% of customers belong to fewer than three **loyalty programs**; these choosy loyalty members want discounts (51%) and engagement rewards (44%).
- **Pay-by-phone:** 48% of drive-through customers, 46% of take-out customers, and 31% of in-restaurant diners want the **pay-by-phone** option.
- **Self-serve kiosk:** Within a QSR, when technology such as a **self-serve kiosk** is used to place an order, visit frequency increases 6% and average spend per visit increases 20%.
- **Feedback:** 84% of customers return if a restaurant responds directly to their **feedback**.

DON'T GET BURNED

Some restaurants and similar merchant brands are engaging CX agencies and technology providers. But the rush to implement this digital transformation could backfire—opening up big risks to the brand, to their business, and even to their customers.

As it is, restaurants are already dealing with rampant network vulnerabilities and risk. We can all name several well-known restaurants that have fallen victim to a data breach of their network. Introducing additional restaurant technology to an already underprotected network only increases the cybersecurity risk, which ultimately leads to lost revenue, along with negative customer experiences and negative online reviews.

And then there's the growing risk of ransomware,[2] which can bring restaurant operations to a halt until the systems can be recovered. Not to mention big ransom fees and the real possibility of repeat attacks.

What's needed is a wholistic view of the technology architecture in place at the restaurants—keeping in mind not just the CX, but also the potential unforeseen pitfalls in network resilience, security, and scalability.

One question for restaurants is: Who is orchestrating all the moving digital components, ensuring that they're deployed successfully, are fully scalable, and do not negatively impact other functions? All these digital transfor-

mative elements rely on one thing: the restaurant's network. What was previously a fairly simple network architecture—a back-of-house segment of computers and a front-of house POS system—now is not only much more complex, but absolutely crucial to the day-to-day operations and success of the business. This highly leveraged network infrastructure is the foundation of the digital customer experience.

KEY INGREDIENTS

Resilience

Let's start with the basics. As restaurants build out more digital customer experience components, they rely more heavily on their network's performance. As if keeping the POS up-and-running and processing credit cards weren't difficult and expensive enough, now restaurants must account for the "always-on" capability beyond the Cardholder Data Environment (CDE).

Ask yourself: *Are my restaurant merchant customers implementing circuit monitoring and automatic 4G cellular failover so that not uncommon incidents such as ISP performance hiccups and temporary outages don't grind their business to a halt?*

Compliance

Merchant businesses, and restaurants in particular, are notorious for struggling to fully meet the ever-evolving but very important PCI DSS (Data Security Standard). Currently at version 3.2, with more stringent policies coming in February 2018, most restaurants lack on-site IT staff and adequate cybersecurity resources to gain and maintain compliance on their own. As additional technologies are deployed, network ports are opened, and third parties are granted remote access, managing PCI compliance gets a lot tougher.

Ask yourself: *Are my restaurant merchant customers giving PCI DSS ample attention? And are they working with a managed security service provider that can both help meet the security requirements and support the merchant in validating and reporting compliance as required? Is this provider able to support EMV and P2PE technologies as well?*

Security

Although PCI DSS compliance offers a baseline level of security, given the continually increasing instances of data breaches, it's all too obvious that advanced threat protection (ATP) is sorely lacking. With every new technology implementation, a new threat vector is introduced for malicious hackers to exploit and for employees and vendors to mishandle.

In 2017, tremendous breakthroughs made ATP accessible to merchants of any size. ATP solutions are available as software or as managed services, and differ in approaches and components. But most include some combination of endpoint agents, network devices, email gateways, malware protection systems, and a centralized management console to correlate alerts and manage defenses.

Ask yourself: *Are my restaurant merchant customers deploying ATP at every location, and at every terminal and mission-critical device?*

Franchise Network Standardization

For franchise-model brands, there is an added layer of complexity. Just identifying and implementing effective network standardization and cybersecurity are not enough to protect the brand. And trying to wrangle hundreds of franchise business owners is like trying to herd cats. A change management strategy to effectively communicate, organize, and shepherd a standardized security program into all franchise locations is a must.

Ask yourself: *Are my restaurant merchant customers prepared to effectively roll out a network standardization initiative for their brands across the franchise?*

MEET THE EXECUTIVE CHEF

These are just the base ingredients of a digital customer experience for restaurants, yet the base ingredients make the dish. So, who is best suited for the role of executive chef? This requires someone who has a close relationship with the restaurant, coupled with a broad view of the technologies required. Retail solution providers best match that description and, through key partnerships, can bring together these ingredients—network infrastructure resilience, compliance, and security—to help restaurants ensure that their CX vision enables continued business growth and success.

THE RIGHT TOOLS

To serve up the best digital customer experience, the tools matter. Retail solution providers should be able to provide these key solutions:

- **Managed firewall service:** a first line of defense to protect the perimeter of the network; includes network segmentation, and is compatible with P2PE and EMV
- **Circuit monitoring and failover:** a service crucial to making sure that the network is performing well and can seamlessly switch to another connection, which ensures business continuity
- **PCI DSS compliance management:** a comprehensive solution that provides the ability to validate compliance and manage vulnerability scans; includes file integrity monitoring and consultative support
- **Advanced threat protection:** an actively managed solution to defend against sophisticated malware and hacking-based attacks that target sensitive data on critical endpoints such as the POS

With digital transformation initiatives quickly becoming a necessity in the restaurant industry, retail solution providers are in a unique position to give their merchants a successful experience—by ensuring that the most fundamental component (the network infrastructure), is secure, resilient, and compliant. **c**

---

[1] From "The restaurant of the future: Creating the next-generation restaurant experience": https://www2.deloitte.com/us/en/pages/consumer-business/articles/restaurant-future-survey-technology-customer-experience.html

[2] See "Point-of-Sale System Ransomware: Is your business prepared for the next big threat?": https://www.netsurion.com/solutions/advanced-threat-protection/pos-ransomware