Deloitte.

How restaurants can better manage cyber risk in the extended enterprise

Turning the tables on cyberattacks

The risk of cyberattacks and security breaches is a critical concern for restaurant executives. It's also a heightened area of focus for boards. How can executives help their companies better anticipate and manage cyber risks? Where are restaurant companies most vulnerable? How can they advise their boards on key issues and developments in this increasingly complex area? And how should companies consider the impact of broader enterprise risk?

Evolution of the restaurant extended enterprise

Restaurants are implementing innovative technologies and adjusting their business models to enhance the customer experience, strengthen sales and margins, and improve operational efficiency. Some of these innovations involve technology enhancements to point-of-sale (POS) systems, new cloud-based technologies, and an ever-increasing number of third parties that interact with customers. New business relationships and processes can create security gaps, alter access to sensitive data, or cause shifts in cyber risk liability exposures.

Customer experience – Access in a digital environment

The days of calling a restaurant for reservations may soon be over. Customers now have real-time visibility into table availability and can book a reservation with one click on their mobile devices. Restaurants are heavily dependent on reservation apps to remain front and center with customers and satisfy a key logistical need—increasing traffic and managing table-turns. Loyalty programs are also being integrated with reservation systems to capture ever-more sensitive customer data.

Additionally, the on-demand nature of customer preferences has given rise to new services, such as food delivery, that were previously limited to specific niche segments of the market. A number of third-party delivery providers are now accessible via mobile device apps and have access to a wealth of customer data, including payment information.

In many cases, restaurant reservation and delivery platforms are not integrated with a company's point-of-sales system. Restaurants access data through companies that provide these platforms and may not have knowledge of how their data is securely stored, segregated, and transmitted. For example, reports may be sent to restaurants via traditional spreadsheet extracts from third-party systems. Reservations and delivery are not new ideas, but the manner in which they are being embedded into the digital restaurant experience has fundamentally changed—and opened up access to critical customer data to third parties that now broker these transactions. These third parties also may be sharing or storing sensitive data with other third parties unbeknownst to the restaurant, which creates new vulnerabilities and entry points for cyberattacks and requires greater vigilance to protect key customer data.

Recent innovations like tableside technology and kiosks also allow customers to place orders and pay without the need for employee interaction. These new types of devices are enhancing the customer experience and operating efficiency by accelerating activities that customers typically want to expedite (ordering and paying). These self-service technologies, which may be managed and owned by outsourced providers, are capturing volumes of data about customers—from general profile information like home address and dining preferences, to sensitive data like credit card information taken during the payment process.

Payments – Evolving technologies

The payment processing industry is continuously evolving with consumers demanding more convenient and flexible options. This shift incorporates an innovation-driven ecosystem consisting of processing terminals, new mobile technology, and credit card companies. Each generation of payment technology—from the traditional magnetic stripe cards, to chip cards, to various derivations of mobile contactless methods—has provided significant business benefits. But it also introduces new cyber risks.

The latest Europay, MasterCard, and Visa (EMV) standard, also known as "chip-and-pin" and long used throughout Europe, became an industry standard on October 1, 2015. The October 1 deadline was not mandatory for processing payments; rather, it was a deadline where the cost of fraudulent transactions (using the magnetic stripe cards) would be shifted to the merchant, rather than the credit card company—a potentially catastrophic financial event for small merchants. While EMV cards are viewed as a step to decrease credit card fraud, the ability to accept EMV cards does not come cheaply as they require new terminals capable of reading the embedded chips—however, restaurants must also consider the cyber risks of not upgrading.

While traditional card methods have evolved, other payment innovations that completely eliminate the physical use of a credit card have emerged as a convenient method of payment for customers. For example, one new technology expected to see wider adoption is contactless payments enabled by Near Field Communication (NFC), which allows customers to process and authenticate a transaction using their mobile devices. Much like the EMV standard, innovations in payment technologies should be viewed as another step along the payment security infrastructure. Therefore, strengthening resiliency to cyber breaches associated with new payment technologies can be essential to business continuity.

Putting it all together

Recent cyberattacks suggest that restaurants may be prime targets for criminals and others looking to cause irreparable damage to companies through the exploitation of sensitive data. The use of new technologies, and the fact that restaurant companies process millions of credit card transactions annually, increases susceptibility. The core issue is that a greater number of third parties are handling an increasing amount of sensitive data. Recent high-profile cyber breaches only highlight the urgency for restaurant companies to contend with cyber risks to protect their customers, brand, and operations.

How, then, can restaurants turn the tables on cyber risk? By expanding their cybersecurity programs to also detect unauthorized activity and respond effectively when incidents occur. Rather than focus solely on security, restaurants should develop strategies for becoming *Secure. Vigilant.Resilient.*

Putting *Secure.Vigilant.Resilient.*™ on the menu

Secure.Vigilant.Resilient. is Deloitte's three-course approach for controlling cyber risk. Companies should build a core security foundation by establishing controls and processes around their most sensitive assets, including staying current with technology vendor patch updates. A 2015 Verizon study found that companies are vulnerable when they don't act on improving known weaknesses in their environment. In fact, "99.9 percent of the exploited vulnerabilities were compromised more than a year after the Common Vulnerabilities and Exposures were published." [1]

1 "2015 Data Breach Investigations Report," © 2015 Verizon.

With respect to being vigilant, companies must maintain awareness of how threats are evolving and be able to detect malicious or unauthorized activities. To that end, many organizations are making use of Security Information Event Monitoring (SIEM) technologies to provide insights on threat activity and support monitoring and advanced detection capabilities that focus on critical business processes.

Being resilient is the ability to return to normal operations quickly to reduce the impact of cyberattacks and breaches. This means having the capacity to rapidly analyze situations; execute business continuity and recovery plans; and interact effectively with customers, media, legal counsel, law enforcement, and industry peers. Leadership must be equipped to take quick and decisive action, even when faced with an incident it may not be fully prepared for.

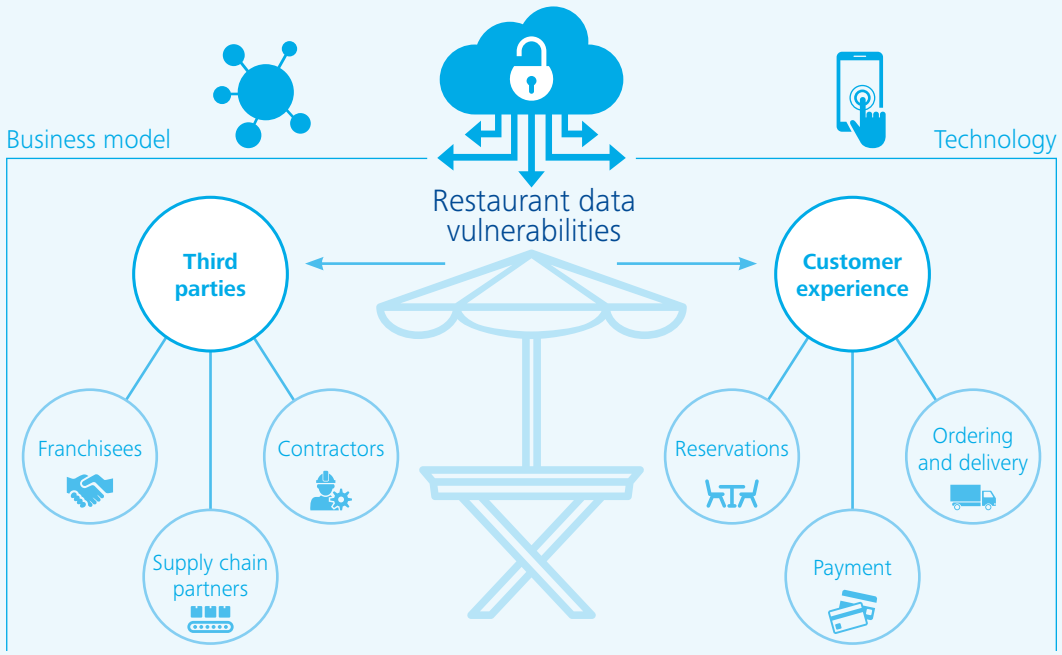
Secure.Vigilant.Resilient.™ Cyber Risk Program

The cyber risk program is executive-led and is continuously adapted to shifting business strategies and the evolution of cyber threats.

Securing the restaurant industry against increasing vulnerabilities

The rise of the "Millennial" demographic has spurred investments in technology to enhance the customer experience, and, as a result, a niche of specialized third parties has emerged to create digital solutions. The increased access that restaurants have provided within their extended enterprise to third parties, such as franchisees, logistics companies, and cloud-services technology providers, has created increased data security vulnerabilities.

Extended enterprise: Data protection challenges in a digital era



A highly competitive environment is causing many companies to revisit their business model to find new growth opportunities, such as franchising/refranchising. The drive to improve margins and a renewed focus on operational excellence also has led to an increased use of contractors and outsourcing. Restaurants have expanded and diversified their use of third parties to provide additional services to their customers. However, as the number of third parties increases, managing the risks of outsourcing services as well as the information systems risks associated with each third party grows in complexity.

Laws and regulations are constantly evolving, and there has been an increased focus on third-party risk management. Consumer protection agencies like the Federal Trade Commission (FTC) have successfully brought suit against franchisors for data and security breaches at its non-owned franchised locations. This means data and privacy vulnerabilities are multiplied as data collected throughout the entire system of owned and non-owned locations are at risk. This risk extends to franchisee-operated restaurants, corporate offices, and systems for which franchisors may have limited visibility and oversight.

As organizations continue to accelerate outsourcing, effective third-party management can be a complex challenge. Organizations need to be aware of the risks associated with engaging more third parties and take proactive measures to reduce the potential impact to organizational assets. As a result, organizations should adopt a third-party management solution that can:

- Strategically streamline third-party management processes and practices
- Identify, evaluate, and manage all third-party risks, in particular cybersecurity risks
- Comply with legal and regulatory requirements (e.g., Franchise Disclosure Documents) to reduce or avoid regulatory scrutiny of third-party relationships
- Shift the organization's focus from breach and incident response (reactive) to a well-defined third-party management strategy (proactive)

Vigilance – Adapting to changing risks in today's restaurant environment

Technology and growth trends underlying the restaurant industry carry one strong message when it comes to data security: increased access and points of vulnerability. Decisions such as deploying new technologies, granting access to third-party providers, and onboarding franchisees complicate the task of data security in the extended enterprise. Eliminating cyber risk in this evolving environment is not possible, but being vigilant about vulnerabilities in the extended enterprise will help restaurant companies manage them.

The biggest weakness with data security in the restaurant industry is the human component. After all, it is an industry that is heavily reliant on lower cost labor; often experiences high turnover; engages with a variety of third parties, including outsourcers; and directly interacts with customers through various physical and digital venues. This complex extended enterprise makes cultural awareness of data security important not only at the corporate level, but also at the store level and with third parties with whom restaurants engage.

For example, restaurants often move to adoption of new security measures because of regulation, such as Payment Card Infrastructure (PCI). While PCI compliance is an important safeguard for the protection of credit card data, restaurants often view the standards and resulting compliance as sufficient. In many restaurants, it's common for credit cards to leave a customer's sight since they might be processed at a POS station and use of tableside processing isn't yet widespread. Over-the-phone credit card transactions are also still common when processing catering or takeout orders.

Cyber assessments should not be limited to what falls within the scope of compliance, but rather take a holistic view of the digital ecosystem that now connects an entire business with customers, franchisees, and other third parties. Compliance is often focused on testing a set of predefined business processes, whereas cybersecurity should be about building dynamic awareness that moves in lockstep with innovation, business transformation, and emerging cyber risks. An effective cyber program should continually innovate to protect critical assets against known and emerging threats across the enterprise. A critical step is to identify vulnerabilities jointly with third parties, fully understand measures third parties have in place to protect against those threats, and establish monitoring measures that provide early warning signals of breaches in the extended enterprise that may impact the organization.

Resiliency in an extended enterprise

Resiliency is strengthened by the appropriate tone at the top, and through a strong governance structure that includes an awareness of cyber risks at the board level. The culture of treating cyber risk as both a business and technology risk is one that needs to be reinforced through executive-level sponsorship and proliferated throughout the company's extended enterprise. The cultural reinforcement of cyber risk management requires both a wide and deep view to adequately cover third parties that handle sensitive information and employees tasked with safeguarding this information on a daily basis. It may often be viewed as a technology issue, but many breaches occur because proper security measures weren't implemented, either from insufficient (human) vigilance or a conscious business decision to not make certain investments in people or technology.

Allowing employees, business partners, franchisees, and contractors to access systems can be vital to day-to-day business operations. Yet many risk exposures and breach incidents are linked to third parties.

Unfortunately, the information technology (IT) function is not typically consulted when non-IT third parties are engaged. If a cyber exposure is related to a third party and IT was not involved in due diligence, the company can face unknown vulnerabilities.

Another potential concern is insider risk. Disgruntled employees or suppliers with sensitive operations knowledge could potentially inflict damage. Therefore, access to personally identifiable information (PII) should be granted only on a need-to-know basis, and background checks should be required for anyone who accesses PII. As with PII, sensitive data (e.g., food preparation techniques, quality specifications, or development plans) should be defined and protected. Sensitive data should also be segregated from other data and user access properly controlled, and measures such as encryption should be considered.

Executives can gain a better understanding of where there may be cyber vulnerabilities in their extended enterprise by asking certain questions:

- Are our technologies supported by current security patches and standards?
- Is data shared with third parties or stored in nonintegrated systems secured?
- Have the cyber business continuity and incident response plans been assessed?
- What measures must be implemented to safely deploy new technologies, and have they been independently security tested?
- Where is cloud data stored? Who owns it? Who can access it?
- How is data and systems access granted to franchisees, delivery service providers, supply chain partners, and other third parties controlled and monitored?
- What data can employees and contractors (and their employees) access and how are their activities monitored and managed?

In general, perhaps the mantra should be: Trust, but monitor. Once businesses have established a trusting relationship with third parties, ongoing and regular monitoring is key to ensuring that continued trust is warranted and that the organization has the appropriate measures in place to enhance resiliency, including mitigating the impact of potential liabilities.

Reporting to the board

Boards have a general obligation to oversee the systems that mitigate risk to the company's business operations. From an enterprise risk standpoint, the board should be aware of the sourcing strategy and risk that strategy brings and confirm that the risk is sufficiently managed. Given the technical nature of cybersecurity, executives should make a concerted effort to communicate program updates, remediation efforts, and recent incidents to board members. This can help the board focus on enterprise cyber issues that could impact the organization's ability to accomplish stated business goals and strategic objectives.

Driving cyber risk awareness up, down, and out

Bringing the cyber risk conversation to the table is becoming increasingly important, and not just because regulations require it. Customers and the marketplace as well are demanding that organizations that handle personal and sensitive information be secure. But ironclad protection against cyberattacks and breaches is impossible, and no company is immune to cyber threats.

The best plan of attack? Keeping cyber risk on the menu by integrating cyber awareness into the business strategy. And by taking advantage of every opportunity to drive awareness of risk:

- Up to the board
- Down through the organization
- Out to franchisees/licensees, third-party logistics services, supply chain partners, IT/cloud services providers, and other third parties

Establishing the risk appetite for the organization and leading a discussion that frames cyber risk as business risk can help executives design a tailored program that balances the needs for security, vigilance, and resilience. This can also help support, rather than hinder, the agility of the organization to respond to emerging threats.

How Deloitte Advisory can help

Deloitte Advisory offers a complete portfolio of advisory and managed services to help complex organizations identify cyber vulnerabilities, design and implement *Secure. Vigilant.Resilient.* programs, and assist in the ongoing monitoring and adaptation of programs as their business and threat environments change.

Contact us

To learn more about *Secure.Vigilant.Resilient.* services for the restaurant industry, contact:

James Cascone
Partner | Deloitte Advisory
Global Restaurant Leader
Deloitte & Touche LLP
+1 714 913 1056
cjcascone@deloitte.com

Bethany Larson
Partner | Deloitte Advisory
Cyber Risk Services
Deloitte & Touche LLP
+1 612 397 4190
belarson@deloitte.com

Acknowledgments

The following individuals have contributed to this paper:

Matthew Lew, Senior Manager | Deloitte Advisory, Deloitte & Touche LLP

Jacob Gregg, Senior Manager | Deloitte Advisory, Deloitte & Touche LLP

Beth Ruck, Senior Manager | Deloitte Advisory, Deloitte & Touche LLP

www.deloitte.com/us/restaurants