As new technology is developed, and shoppers become more tech savvy, retailers are shifting their channel strategies to work seamlessly together to support the brand and experience. With this shift toward omnichannel comes a variety of options for shoppers to interact with retailers. Whether these customers want to shop online through their computers and mobile devices or at physical stores, organizations are rushing to make the experience as continuous as possible from channel to channel. Some new techniques used to encourage this type of experience include allowing customers the ability to share their digital wallet across devices, providing the option to purchase online and pick up in-store, or providing online experiences in the store through the use of Bluetooth technology for alerts on sales and coupons.

The rise in omnichannel has definite advantages for retailers. Omnichannel empowers retailers to track spending and tailor their marketing programs to their individual consumers. This shift has led to the rise of big data within retailers as well as introduced new technologies, such as Responsive Online Ordering systems or Bluetooth store sensors. These new systems are being used to revitalize sales and launch typical brick and mortar retailers further into the 21st century; however, these new systems also introduce new attack surfaces that retailers may not have previously considered.

With the rise in omnichannel presence and the need to protect a variety of new technologies and concepts across all retail subindustries, it is important for organizations to ensure that they have an expandable security program to protect customer, applicant, financial and employee data. To date, retailers have not appropriately allocated resources to address the security of data not related to payment card industry (PCI) needs, but they are starting to shift the focus. It is critical that retailers continue that shift while adopting a security framework that focuses on reducing risk in the way the organization conducts business processes and handles technical security risks.

Omnichannel and its impact on security

Omnichannel was introduced into the marketing and retail world in 2010 but many middle market organizations are still rolling out their strategies. Those further along continue to identify and adopt new technologies to facilitate the experience.

These new processes have increased the amount of data being collected, stored and used to make decisions to grow the organization. For example, when working with a middle market grocery chain, RSM’s team identified that the company was collecting data on shopping habits, birthdays, checking accounts, family members and more as part of a new version of their loyalty program. Over the six months that the process had been in use, the chain had collected information on more than 1 million customers.

The loss or compromise of any of this data could have had massively detrimental financial and reputational impacts on our client. At the time of the assessment, the organization had minimal controls, spending most of their resources (dollars and time) on PCI compliance, while neglecting the other data sets. Multiplying the average dollar loss of a record of this type by the number of records that were available to compromise, this organization was looking at a single loss potential of more than $158 million. In an industry that averages 1 to 2 percent profit margin a breach of this data could sacrifice profits for years to come. This doesn't even begin to cover applicant and employee data, which amounted to more than 15,000 applicants through the first six months of 2016 and more than 2,000 employees.

The collection of these data sets and introduction of each new technology brings unique challenges for security departments within retailers. These challenges must be solved in order to ensure that the organization truly understands and mitigates risks to the extent possible in the deployment of these solutions.

---

Reducing the risk of omnichannel

To date, RSM’s work with retailers has highlighted the need to place more emphasis on security within the organization beyond PCI compliance and the protection of cardholder data. Many of our clients spend less than 50 percent of their budget to specifically secure other portions of the organization. In fact, several of our clients even limit the scope of penetration testing to just their cardholder data environment (CDE). This scope limitation is indicative of the lack of protections on the rest of the organization that could have an impact on financial, brand and reputational risk factors. However, while our assessments often find a lack of non-CDE security, our work shows that many retailers believe the opposite. Many spend more than 50 percent of their budgets on efforts outside of PCI compliance. This might be a sign that some organizations are beginning to mitigate the risk of non-PCI data.

Regardless of any shift, most retailers have not provided security a seat at the executive level, relegating the most senior role with dedicated responsibility for security several levels below the executive team, according to the survey. This decision alone makes any efforts to branch out from the CDE effectively very difficult. In talking with several retailers who lead their respective organizational security programs, we have learned that this likely occurs because the typical approach has been to make security an IT problem. With the emphasis on securing the network, applications and infrastructure, the relevant skill sets tend to be found within IT. However, relegating security to implementing a few technical controls belies a fundamental misunderstanding of how security incidents can affect an organization. Following this approach, security has centered on incident response (IR), system monitoring and a general atmosphere of fear, uncertainty and doubt.

Technical controls and IR capabilities are important, but in order to truly reduce risk, security should be embedded in how organizations do business. Working to reduce risks in the performances of critical processes will continue to support the business goals while improving overall security. For example, a process within a large retailer with more than 1,000 locations focused on specialty items; within their marketing department, the organization uses multiple databases with the same customer sensitive information to process and analyze data. Not only does this lead to integrity issues with no single source of record, but the multiple storage points for data can lead to increased costs for encryption and other security controls, inflating security budgets without actually addressing the problem. All it would take is one person with legitimate access to decrypt the data for everything to be compromised, which would be a disaster for the company.

Six steps to evolving security for omnichannel

For middle market retailers, omnichannel strategies are still in their infancy and will continue to grow. This means that security departments within these retailers can continue to evolve their security strategies to meet the growing needs of the organization and enable growth for the business. There are six critical components that allow retailers to securely increase relationships with their customers and meet their ever-changing needs.

1. Develop a partnership with the pacesetters
Marketing is often the driver in most organizations when it comes to omnichannel efforts. Case in point, we interviewed the director of marketing and e-commerce for a Fortune 1000 restaurant chain recently regarding omnichannel initiatives. Through our discussion the director revealed that marketing often moves so fast to adopt new technologies that the company’s security team is sometimes unaware of all upcoming initiatives. While the omnichannel driver may not be the marketing team in all companies, the security group at each organization needs to identify those with the most velocity for driving corporate growth, the pacesetters, and develop a strong line of partnership and communication with them. For security leaders who are positioned below the executive team, the challenge becomes balancing day-to-day responsibilities with the push to meet with and develop relationships with those higher on the corporate ladder. To build these relationships, security leaders should focus on setting up consistent meetings to discuss direction and learn more about their counterparts, injecting themselves early into projects to identify and communicate the risks, along with the remediation recommendations.

2. Improve and expand the security workforce
While developing a partnership with the pacesetters, security leaders need to make sure they get the right team on board. Security leaders are often promoted through the ranks of IT, and these individuals need to either seek education to increase their business knowledge or hire individuals with experience in working with business processes. Securing processes requires the ability to facilitate discussion on how the company conducts business. Using these discussions, security leaders should identify process flows and narratives and determine process improvements, focusing on efficiency while providing a strong foundation to support the technical members of the security team. These members of the team can work together with the rest of the company to develop and re-engineer processes in a secure fashion that meets the goals of reducing scope and complexity before adding security controls. Furthermore, business analysts (or those with the process level expertise) can bring a unique perspective to security, focusing not as much on the technology, but on how the business actually functions.

3. Understand the data and process and data flow(s)
With the right training and individuals in place, the security team needs to understand the critical processes within the marketing business function (or other pacesetters). Meeting with members of management who oversee the critical business functions related to omnichannel such as marketing, development, legal, store operations and more can allow security to identify those processes that are critical and prioritize them based on their confidentiality, integrity and availability (CIA). Security needs to focus this effort on criticality of the process to the business and the data within.

Once the processes are identified and categorized, the next step is to conduct process and data flows to understand how the process

---

4 For more information on the CIA Triad, please visit http://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA
occurs. During this step, the security team must walk through the current (or proposed) process, identifying key resources, third parties and applications. The team should also identify all applications, supporting systems and third parties, as well as potential issues with how the process is designed, including items such as unnecessary storage of data, provisioning of users and access, and how data will be processed and shared.

4. Apply process improvements
The outcomes of the process and data flows should lead right into recommendations for process improvements or risk reduction methods. For example, focusing on decisions of insourcing versus outsourcing, data collection and storage, transmission channels, and individual or business groups with required access can often provide a great reduction in overall risk. For those used to working closely with PCI data security standard (DSS), follow the process of scope reduction and applicability as a general method for process improvements.

For example, RSM worked with a manufacturer and retailer of medical supplies to review a process focused on ordering and payment for the supplies through an e-commerce platform. As part of their business practices, this organization collected more information than required including full health records (which included insurance providers, dates of birth and Social Security numbers) regardless of whether the buyer was paying with insurance or some other form (credit card or automated funds transfer). The owners of these processes determined that only 50 percent of customers needed to provide the information, meaning that the other 50 percent of customers were submitting excess data. Working then with the security team, internal audit and process leaders, the group identified ways to limit the amount of data they were collecting (based primarily on payment type), and transferred the risk of credit card processing through the use of an iframe. This effectively reduced the risk posed by the process by more than 80 percent and the cost of compliance by limiting the control set needed to protect the data.

5. Implement security controls
Once the process improvements are completed, technical controls can be applied. Based on the newly limited scope, controls should be selected based on alignment to a specific and relevant framework encompassing all regulatory and contractual obligations. For example, most retailers still have to comply with PCI DSS, so those controls need to be accounted for. Other organizations have additional frameworks and regulatory considerations such as the Sarbanes-Oxley Act, Health Insurance Portability and Accountability Act and other state and national privacy and data breach requirements to meet.

To develop the framework, companies should seek to perform an exercise with internal audit, IT and security to ensure that all applicable controls are considered. Alternatively, these companies can seek external support with the use of consultants or framework mapping tools like the Unified Compliance Framework. Ultimately, most organizations will map to the National Institute of Standards and Technology Cybersecurity Framework or International Organization for Standardization ISO frameworks.

Based on the full control set, each process should apply controls related to the risks associated with the process (confidentiality, integrity and availability) similar to those within the Federal Information Process Standards 1999 (FIPS 1999) process used by government entities for Federal Information Security Management Act compliance. High risk processes would receive the full control set, while moderate and low risk processes would receive a subset. It is also important to take into account control applicability (i.e., no need for storage controls for processes that are not storing).

6. Embed security in technology
As mentioned earlier, omnichannel efforts focus heavily on advancing technology, such as newly integrated mobile and web applications, web services connections, Bluetooth technology, line-breaking kiosks and mobile devices, store pickup vending machines and much more. As the technologies continue to evolve, the security team must find unique approaches to secure these technologies. Some options that security teams may consider include:

Application architecture reviews
Early in the development life cycle, security teams should perform an application architecture review to identify how security should be integrated within an application. While this likely cannot be integrated into all development, focusing on the highest risk and strategically critical applications will provide the most insight. The application architecture review process should encompass reviews of proposed data flows, third-party service calls that must be made and the security controls present within the application. Furthermore, attack modeling, which focuses on the identification of threats and how those threats would attack the application, should examine how exploitation may occur upon those missing controls, including:

- Identification and authentication
- Authorization
- Access controls
- Data integrity
- Cryptography and key management
- Logging and monitoring

Third-party vendor management
A natural byproduct of developing process and data flows is the identification and assignment of risk to vendors and partners who facilitate omnichannel efforts. This should help in the development of a vendor contract management program that ensures a vendor is vetted (from a security perspective) before the contract is signed. This will provide an understanding of how the organization is being protected, ensuring the contractual language appropriately enforces the requirements for security.

In our work with clients, we have found that while clients have many of their vendors in some type of program, it is not usually all-encompassing. Furthermore, contractual language is often applied in a blanket fashion, which does not specifically address how certain data elements should be handled and protected.

Traditional security testing
In addition to the unique ways to approach the advancing technology, traditional security testing and controls implementation need to be continued (see chart on p. 4). This

---

means hardening the operating systems, using secure coding practices, granting access on a minimum required basis, logging and monitoring appropriately, and testing based on the in-scope technology. This is a practice that most organizations have implemented.

Summary

Even after any changes have been implemented, some risk will remain. This residual risk is what cyber liability insurance is designed to cover. While your organization may decide not to cover all risks with insurance, it is important to understand what may remain outside an insurance policy, related costs and have discussions with the executive team about those potential exposures.