IDC ANALYZE THE FUTURE

IDC MARKET SPOTLIGHT

Sponsored by: Cisco

Digital transformation (DX) in the retail industry is changing how retailers do business, and security strategy needs to keep pace with DX, with continuous enhancement and innovation in the security resources and organization, security processes, and security technologies within retail enterprises, both small and large.

Reassessing Retail Security Strategies and Portfolios for Today's Challenges

May 2020

Written by: Robert Eastman, Research Manager, IDC Retail Insights

Omnichannel Security and Digital Transformation

Digital transformation (DX) is equipping retailers with both current-state and future-ready digital tools, practices, and technologies necessary to offer an immersive, pleasant, and convenient customer experience in every channel and across all touch points. Digital transformation is changing how retailers do business, how they innovate, and how they engage with their customers.

The modern retailer must be data driven, continually innovative, and relentlessly focused on delivering the best possible customer experience. Digital transformation is the foundation for deploying the necessary technologies and adopting the necessary practices. IDC research has identified 56 prominent retail digital transformation use cases within five strategic retail priorities: omni-channel commerce, curated merchandise life-cycle management, omni-experience customer engagement, digital supply chain optimization, and operational scale and agility.

AT A GLANCE

WHAT'S IMPORTANT

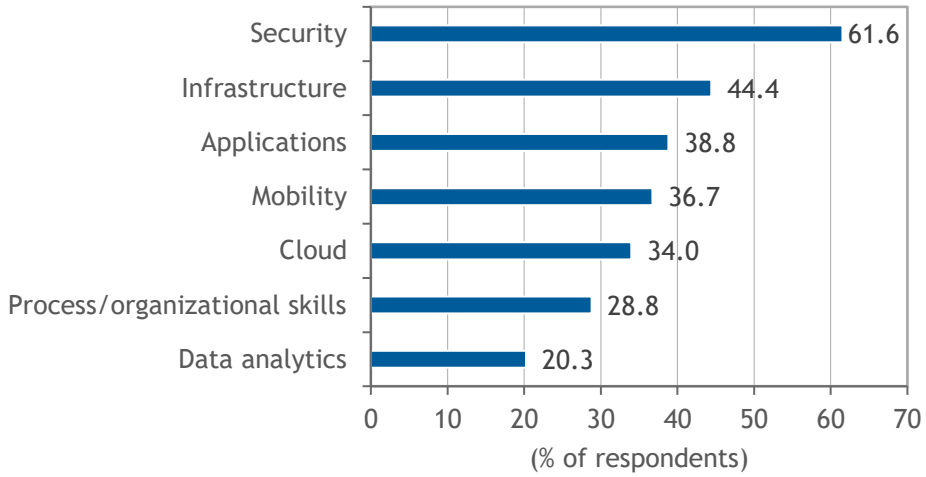
Digital transformation is forcing retailers to reassess their security strategy and security technology portfolios and take advantage of a continuing stream of improving security technology. At a time when the retail industry's attack surface is growing and the list of threats and threat types is getting longer, retailers need to deploy security solutions with better manageability, automation, and orchestration in order to mount effective defenses.

Leveraging digital transformation in the deployment of these use cases, retailers are delivering on their experiential retail mission to continually innovate around the customer experience. Retailers that embrace digital transformation will be in a much better position to discover and leverage points of competitive differentiation to become retail leaders.

Among the many drivers for retail digital transformation, retailers are finding the particular DX use case or use cases that deliver the most benefit. Importantly, in this period when cyberthreats are growing in number, adaptability, and sophistication, security emerges as the top IT area where retailers need to make investments or changes when undertaking digital transformation (see Figure 1).

FIGURE 1: ***Investments Made in Response to a DX Project***

Q ***Which of the following IT areas were the largest investments and/or changes made in response to the digital transformation (DX) project?***



n = 150

Source: IDC's Digital Transformation (DX) Executive Sentiment Survey, May 2018

The new data-driven retailer is leveraging digital transformation because it recognizes that digital must be the basis for everything that the enterprise does. Business processes, people, assets, and technologies must be digitally connected. Digital must be the basis for how the company operates, how the company innovates, and how the company engages and delivers products to customers. This is leading to an explosion of new and emerging technologies that span the range of business functions for the retailer. With this adoption of more and more technology has come an explosion of data from systems across the enterprise. The Internet of Things (IoT) will only accelerate the explosion of data.

With digital transformation, and the adoption of more and smarter technologies inside the store, retailers have seen a dramatic increase in the retail attack surface. The list of threats is long and growing longer. With the arrival of IoT, the adoption of edge computing, and the move to the cloud, omnichannel security becomes much more complex for the retailer. When business conditions take an unexpected turn, as the industry is now experiencing, security is at risk of becoming an afterthought just when threats are on the increase.

At the same time, the operational side of the house is getting smarter. Retailers are installing smart lighting, smart HVAC, and other building controls, and IoT is making inroads to make building automation smarter. The assets that used to be air-gapped are now vulnerable connected assets. IT and operational technology (OT) can no longer safely be siloed security domains. The increasing adoption of IoT will require retailers to allocate more budget to the protection and defense of their IoT assets.

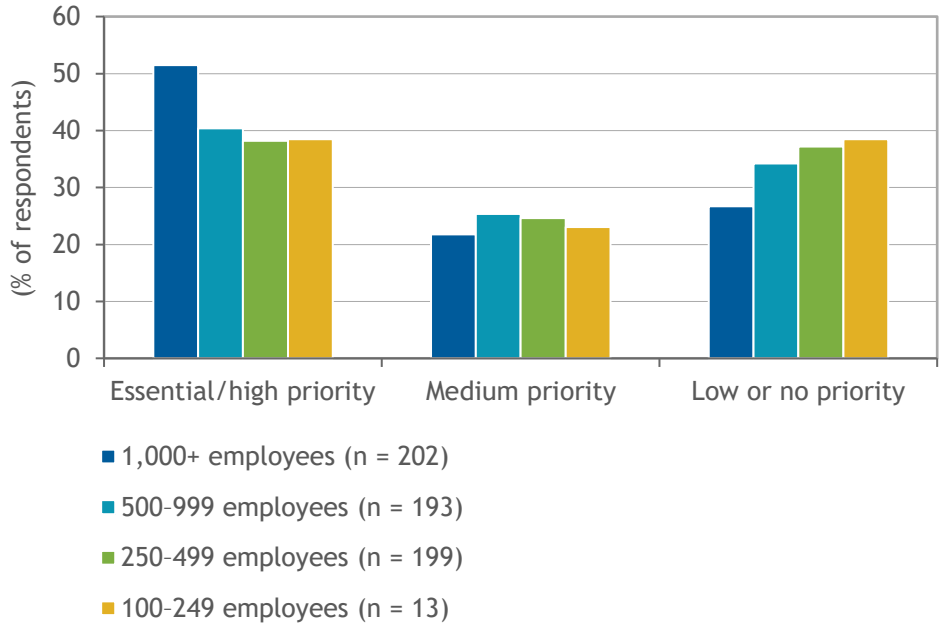
SMB Retailers and Franchise Retailers

The security problem becomes even more acute for small and medium-sized business (SMB) retailers and franchise retailers that have an even more difficult time allocating attention, resources, and the right skills to address the issue, much less keep up with the cyber arms race.

When a 2019 IDC survey asked retail organizations about the priority level for security over the next 12–24 months, the larger retailers reported allocating more attention to omnichannel security (see Figure 2).

FIGURE 2: ***Prioritization of Security by Retail Organizations***

Q *What is the priority level of secure omni-channel operations in your overall innovation effort over the next 12–24 months?*



Source: IDC's Global Retail Innovation Survey, May 2019

In the smallest retail organization segment in that same survey (100–249 employees), 60% of retailers that indicated security was "low or no priority" said, in fact, that security was not a priority at all. The smallest retail segments — which also include franchise retailers — often do not possess the expertise or bandwidth to understand their security needs or what the market has to offer. Franchisees have additional challenges. Often the franchise retailers are directed to use corporate systems in order to deliver a customer experience that is consistent across locations as well as for purposes of operational efficiency; the cybersecurity protections and practices of the franchisee are often only as good as those of the franchisor. This holds true also considering the franchise retailer is dependent upon the brand, reputation, and marketing — and cybersecurity expertise — of the parent company. Simply consuming services of a parent company means the franchisee's security posture may not be monitored for compliance by the franchisor, which may bring additional financial implications.

State of Omnichannel Security

Worldwide retail spending on security hardware and software is forecast to grow at a five-year CAGR of 8.72% from 2018 to 2023, an increase from the 7.6% CAGR from 2016 to 2021, driven by both the introduction of more smart technologies into the connected store and the heightened sophistication, impact, and visibility of cyberattacks in the retail domain.

The urgency of better omnichannel security is being felt by retailers of all sizes. While there are encouraging signs, such as a shrinkage rate that has remained steady over recent years, other areas of cybersecurity such as organized retail crime (ORC), cybercrime, returns fraud, BOPIS-related fraud, account takeover (ATO) fraud, and gift card fraud, in particular, are becoming more of a focus for retailers.

Retailers — often constrained by lean IT staffs and a scarcity of skilled cybersecurity resources — are responding by layering on solutions to address an immediate tactical need. Without much orchestration or automation, these solutions struggle in the transition, particularly, from detection to response. Retailers are overwhelmed with the volume of alerts, unable to identify the most critical items or react to the most critical threats, and thus are unable to focus efforts, coordinate actions, and optimize responses.

This evolution to converged omnichannel commerce and completely connected retail is creating new opportunities to deliver a better, richer experience for consumers. Unfortunately, this digital transformation is also creating a broader, more digital attack surface for bad actors. The challenge of cybercrime has become an arms race — and a dance. As retail enterprises deploy better security in one area, cybercriminals and other threat actors adapt their methods of attack and move to the next perceived weakest point, which may be an enterprise asset or a shadow IT asset or solution. Reacting to each new attack with yet another security solution has resulted in many retailers deploying dozens of unintegrated solutions, which are acting as isolated solutions to one particular threat. With alarms coming from each of their solutions, security teams are overwhelmed with alerts and are poorly equipped to identify the most critical threats or to mount a well-coordinated response.

Cybersecurity Technologies Grow in Sophistication to Meet the Challenges

IDC's cybersecurity taxonomy encompasses a breadth of solutions across the network security; content inspection; internet defense; endpoint security; identity and digital trust; data security; IoT security; and analytics, intelligence, response, and orchestration (AIRO) categories.

To meet the challenge of critical threats across the IT and OT retail attack surface, retailers must take a broader, more holistic, and more strategic approach to omnichannel security, with a focus on the following cybersecurity pillars:

- **Identity management —** managing identity and account credentials. Identity management, also known as identity and digital trust (IDT) or identity and access management (IAM), addresses not only identity but also legacy authorization, advanced authentication, and privileged access management. Identity is at the heart of security, and, when compromised, it is associated with multiple forms of fraud and other security issues.
- **Trust management —** protecting confidentiality and integrity of data. Trust is an overarching concept describing the condition that enables two or more parties to come to agreement with an acceptable amount of risk; trust management consists of technologies that serve to establish and maintain trust, leveraging IT and usage policies, IT procedures, and such specific technologies as virtual private networks (VPNs), encryption, file integrity checking, and digital signatures.

- **Vulnerability management —** assessing the attack surface. Vulnerability management is the critical capability to continuously scan and assess the attack surface for risks with the objective of identifying, remediating, and eliminating weaknesses in the environment that present opportunities for attack.
- **Threat management —** monitoring activity for suspicious actions and attacks. Threat management monitors usage activity to identify suspicious usage that could indicate activity that is malicious or inappropriate and then react and respond and then recover from security incidents.

Enterprises that implement these pillars in a coordinated manner, rather than in silos, have a much better security strategy and posture than enterprises that implement these pillars in isolation. This approach to implementation is indicative of an enterprise with a high level of maturity in its security capabilities.

While larger enterprises will be better equipped to develop comprehensive and consistent strategies across these disciplines, smaller retailers are more hard-pressed to find the resources — budget and cybersecurity skills — to instill these disciplines across the board. Smaller retailers must allocate their less abundant resources more often to regulatory compliance, data protection, and data privacy.

All enterprises are struggling with managing the mixed and unintegrated portfolio of cybersecurity solutions that they are using, dealing with the often overwhelming number of alerts they are seeing, and with mounting effective coordinated responses. The security technology vendor community is responding with solutions that incorporate more capabilities into their solution sets in an effort to offer more of a platform to retailers. Recognizing the scarcity of skilled cybersecurity resources, security technology vendors are enhancing their solutions, building in better usability, automation, manageability, APIs for integration, and dashboards and other capabilities for sorting through the morass of alerts to focus the right resources on the most critical threats. SMBs in particular need better management and automation for use by lean IT teams stretched to the max. Often SMBs are tempted to use consumer-grade security technology (with the underlying expectation for consumer output functionality) or get by with legacy technology that they deem "good enough." Security vendors today are offering smarter security solutions and technologies that can leverage existing legacy security systems.

When IDC asked retailers about the specific security-related investments or changes they were making as part of digital transformation, they identified the following areas as the top five: security analytics, web security, security and vulnerability management, cloud access security brokers, and network or physical security.

Network security — which includes firewalls, unified threat management (UTM), intrusion detection and protection (IDP), and VPN — is critical for every enterprise; the network is both the conduit for all data in the store and the nerve center of the store — the backbone for digital transformation and nearly every technology investment that the retailer is making. Digital transformation is introducing more complexity into the retail environment, putting added stress on networks. Necessary security silos within the organization and tiers of hierarchy to secure traffic such as running on MPLS versus SD-WAN, for instance, help protect business-critical applications. However, when increasing network complexity is combined with these types of organizational complexity, that can prevent valuable cross-enterprise visibility to security issues, resulting in the risk from security incidents to rise considerably. The near-term arrival of 5G will introduce new network performance opportunities to enterprises and allow for the creation of virtualized networks for specific applications or workloads, putting an even greater importance on the security of network infrastructure.

Unified threat management, in particular, is becoming an attractive option for enterprises, delivering consolidated capabilities (firewall, network intrusion detection and prevention, and gateway antivirus, as well as, perhaps other functions) and form factor efficiency. Retailers in particular need integrated security solutions such that the consumption of threat intelligence has telemetry in the feedback loop with endpoint protection. This ongoing exchange of what's happening in the network, along with detection of any abnormalities, and the subsequent communication back to the provider to carry out the appropriate actions needs to remain consistent, as well as adapt to inevitable changes in the environment and types of security threats.

More than 20% (21.7%) of retailers identified IAM as number 6 on the list of security investment areas. Identity and digital trust (as IAM is now referred to) is central to the concept of security, particularly for hybrid cloud environments. As incidents of ATO fraud, as one example, rise to be a major concern for retailers, security solutions with multifactor authentication for instance will also remain prevalent to support identity and digital trust for retail security strategy.

As endpoints continue to multiply within the retail enterprise — not only more mobile devices, point-of-sale systems, and other peripherals, and tablets but also, increasingly, IoT sensors and devices — endpoint protection and dynamic network segmentation become critical for the retail enterprise.

Data privacy and protection is also becoming a hot button for retailers as they find that consumers are becoming more sensitive to the protection of their data and willing to make retailers pay the consequences of not adequately protecting their personal information. With retailers having to become better at collecting data of all kinds within the retail four walls, both business information and the personal information of customers means that data protection — always important — has become more urgent than ever before. As this issue has been heightened in the minds of retailers and consumers alike, retailers are coming to realize that the challenge of protecting customer data goes beyond meeting GDPR and PCI compliance.

As retailers invest in these and other security solutions, the focus increasingly is on four key control points: identities, applications, data, and endpoints. Leveraging policy-based security measures is becoming increasingly beneficial for retailers that may want business-critical applications (e.g., POS) on their own isolated network. Retailers that converge their security strategy silos and deploy security platforms with better management and automation around the identity management, trust management, vulnerability management, and threat management pillars will be in the best position to manage their security challenges.

The Future of Cybersecurity: Strategic Priorities for Retailers

Digital transformation is changing the way that retailers do business and introducing a wave of new technologies into their enterprises. With this embrace of DX, retailers need to take a fresh look at how they are addressing omni-channel security. In an arms race with threat actors, the two biggest dangers are inaction and ineffective action.

At the same time that retailers are adapting DX to their retail businesses and moving to hybrid multicloud environments, convergence is taking place across the retail enterprise: the omnichannel convergence of retail's physical and online customer channels, the convergence of the IT and OT domains with the expansion of IoT, and the necessary convergence of security strategy across the enterprise. This omnichannel convergence is introducing complexity into their retail enterprises even as security risks and threats morph and adapt to the next best point of weakness in retailers' defenses.

Retailers large and small need to allocate precious IT and scarce security resources across the security functions of protecting data and assets, preventing threats, detecting attacks, and resolving incidents.

Retailers need — and are getting — better manageability and more automation in security solutions. Expanding security platforms will allow retailers to rationalize and simplify their security portfolios, and better API integration will allow retailers to better coordinate security responses across their security portfolio. Artificial intelligence (AI) and machine learning (ML) are delivering much better ability to sense the slightest changes or abnormalities in data, or changes to baseline across a range of security solutions and in fraud detection, but these technologies need to overcome industry inertia and mistrust in delegating decisions to an AI "black box." The increasing adoption of cloud within retail requires a careful understanding of the respective security responsibilities delegated to the cloud service provider and those to be assumed within the enterprise. With the growing adoption of cloud, cloud security gateways (CSGs) are seeing increasing use, helping enterprises manage user access to cloud applications as well as defining policies about what type of data can be uploaded or shared and what features users can use.

Digital transformation is also inviting an increased focus on SD-WAN within the retail enterprise. This technology has the potential for dramatic savings in network traffic segmentation and data network costs. Aggregation, resilience, prioritization, and traffic shaping are features that work alongside a retailer's evolving business strategy. Both network infrastructure upgrades and security assessment are opportunities for retailers to reassess the advantages of this technology — and to investigate offerings from security vendors.

Cybersecurity skills are sure to remain in short supply for the foreseeable future. This shortage heightens the importance of cybersecurity solutions — platforms — that are more easily managed, can be integrated more easily via APIs, and have better dashboards and stronger analytics — including AI/ML. This management capability becomes paramount for SMB retailers and franchise retailers that are constrained by smaller staffs and thus already have too many tasks on their plates.

IDC offers retailers the following advice:

- **Conduct a holistic reassessment.** Now is the time for such a reassessment of the security strategy and execution and how well the organization is structured and equipped for an effective coordinated response to threats.
- **Assess capabilities.** In particular, retailers should assess capabilities in the pillars of identity management, vulnerability management, trust management, and threat management and leverage advanced security technologies to orchestrate a better security posture across these pillars.
- **Assess abilities to filter through volumes of alerts.** It is imperative for retailers to honestly assess how well they can filter through the high volume of alerts, focus the right resources on the most critical threats, and then adjust dials in adjacent security solutions.
- **Look for automated solutions.** For SMB retailers and franchise retailers, it is even more important to look for solutions that deliver more automation and manageability in the security pillars; in view of the scarcity of skilled cybersecurity resources, managed services may make sense.

- **Leverage security solutions with embedded automation.** Retailers should leverage, where possible, security platforms and solutions with more embedded automation. Filtering and responding to the high volume of alerts are among the biggest struggles security teams are facing. Better automation can scan files faster, collect enormous amounts of data from across threat vectors, aid in identifying anomalies, and coordinate response across the security portfolio.
- **Pay attention to compliance capabilities.** Retailers need to pay attention to the regulatory compliance, audit, reporting, and policy and compliance capabilities within their security platforms.

About the Analyst

Robert Eastman, *Research Manager, IDC Retail Insights*

Robert Eastman, an IDC Retail Insights research analyst, delivers research analysis and insights in his Worldwide Retail Technology Strategies program. His coverage areas include retail infrastructure and technologies, retail IT budget and strategy, retail digital transformation use cases for cloud, mobility, payment and POS, and cybersecurity, all within the retail industry context.

MESSAGE FROM THE SPONSOR

Cisco's security approach for retail

A network capable of supporting emerging digital initiatives is a fundamental element of business success. Protecting the network, therefore, becomes just as foundational to a successful digital transformation strategy as the network itself. At Cisco, we're helping organizations around the globe securely transform by integrating market-leading security with their core infrastructure to help protect their entire attack surface. Having an end-to-end secure network allows organizations big and small to achieve significant cost savings and increased productivity while dramatically reducing time to implement new business initiatives in a dynamic market landscape.

Cisco is equipping retailers to seamlessly adopt new technologies that address evolving customers preferences by ensuring data privacy, providing protection against even the most sophisticated cybersecurity threats, and keeping up with regulatory mandates. In the store and online, from connecting your value chain to improving customer satisfaction, bring it all together with the most secure solutions for your retail environment.

IDC Custom Solutions

The content in this paper was adapted from existing IDC research published on www.idc.com.

IDC Research, Inc.
5 Speen Street
Framingham, MA 01701, USA
T 508.872.8200
F 508.935.4015
Twitter @IDC
idc-insights-community.com
www.idc.com