2016 BDO RETAIL RISKFACTOR REPORT

BDO

"Retailers are operating in an era defined by tepid consumer spending and rapid technological change that is revolutionizing every aspect of the industry—from supply chain operations to payment channels and marketing. Retailers must balance keeping pace with evolving commerce channels and maintaining customer privacy and data security in an increasingly complex digital environment."

Doug Hart, partner in BDO's Consumer Business practice

In a Cyber World, a Rising Tide of Risks Abound for Retailers

Despite optimistic projections from economists and retail executives that gains in consumer confidence would propel economic growth at the beginning of 2016, U.S. retail sales have slipped since January. Q1 results further highlight the impact of tepid consumer spending, which remains a top concern for 87 percent of the industry's top players, according to the ***2016 BDO Retail RiskFactor Report***.

Winning retailers are responding by harnessing the power of their digital platforms to offer convenient experiences that appeal to selective and increasingly sophisticated consumers. Driven by demands from consumers, competitors and regulators, the digital reality in the industry has brought to light the greatest areas of risk that retailers face, including cybersecurity. For the first time in the report's history, risks associated with data privacy and security breaches were cited by all retailers in their 10-K filings this year.

While cyber is the top concern this year, retailers also have their eyes on the risks posed by the competitive, regulatory, technological and global trends both online and off that are shaping the retail landscape.

The 2016 BDO Retail RiskFactor Report examines the risk factors in the most recent 10-K filings of the largest 100 publicly traded U.S. retailers; the factors are analyzed and ranked by order of frequency cited.

ABOUT THE BDO CONSUMER BUSINESS PRACTICE

BDO has been a valued business advisor to consumer business companies for over 100 years. The firm works with a wide variety of retail clients, ranging from multinational Fortune 500 corporations to more entrepreneurial businesses, on myriad accounting, tax and other financial issues.

ABOUT BDO

BDO is the brand name for BDO USA, LLP, a U.S. professional services firm providing assurance, tax, advisory and consulting services to a wide range of publicly traded and privately held companies. For more than 100 years, BDO has provided quality service through the active involvement of experienced and committed professionals. The firm serves clients through 63 offices and more than 450 independent alliance firm locations nationwide. As an independent Member Firm of BDO International Limited, BDO serves multi-national clients through a global network of 1,408 offices in 154 countries.

BDO USA, LLP, a Delaware limited liability partnership, is the U.S. member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms. BDO is the brand name for the BDO network and for each of the BDO Member Firms.

For more information please visit: www.bdo.com.

Top 20 Risks for Retailers

	2016		2015		2014	
General Economic Conditions	#1	100%	#1	100%	#1	100%
Privacy Concerns Related to Security Breach	#1t	100%	#4t	99%	#8	91%
Competition and Consolidation in Retail Sector	#3	98%	#1t	100%	#3	98%
Federal, State and/or Local Regulations	#4	96%	#1t	100%	#2	99%
Natural Disasters, Terrorism and Geo-Political Events	#5	94%	#7	96%	#13	87%
Implementation and Maintenance of IT Systems	#6	93%	#4	99%	#7	92%
U.S. and Foreign Supplier/Vendor Concerns	#6t	93%	#6	98%	#4	96%
Legal Proceedings	#6t	93%	#9t	95%	#8t	91%
Labor (health coverage, union concerns, staffing)	#9	91%	#7t	96%	#5	94%
Impediments to Further U.S. Expansion and Growth	#10	90%	#12t	92%	#17	78%
Dependency on Consumer Trends	#11	88%	#9	95%	#6	93%
Consumer Confidence and Spending	#12	87%	#15	89%	#8t	91%
Credit Markets/Availability of Financing and Company Indebtedness	#13	85%	#11	94%	#11	89%
Failure to Properly Execute Business Strategy	#14	82%	#12	92%	#11t	89%
Changes to Accounting Standards and Regulations	#15	76%	#14	90%	#13t	87%
International Operations	#16	73%	#17	86%	#15	80%
Loss of Key Management/New Management	#16t	73%	#19	80%	#16	79%
Marketing, Advertising, Promotions and Public Relations	#18	66%	#25	68%	#24	64%
Consumer Credit and/or Debt Levels	#19	62%	#27	65%	#23	65%
Joint Ventures	#20	61%	#21	76%	#18	74%

Cyber Fears Earn Top Spot on Retail Risk List

Retailers have grown accustomed to headlines around massive cyber incidents, and are fully aware of their burdensome financial and reputational repercussions. This year's finding that all retailers cite cybersecurity as a potential risk to their business reflects a notable shift from the 55 percent in 2011 and 26 percent in 2007 that flagged potential cyber issues.

This universal fear is not without reason. Retailers face, on average, at least eight cyber-attacks per year, with 74 percent of them considered advanced threats, according to research from the Ponemon Institute. To safeguard the constant flow of sensitive data, more than half (52 percent) of those surveyed in our 2016 Retail Compass Survey of CFOs said they upped their spending on cyber in the past year via a broad array of strategies, including leveraging new software security tools (85 percent) and creating a response plan for potential breaches (71 percent). While planning is crucial and can enable a swifter response once an attack takes place, cybersecurity has become a continuous game of cat and mouse, with fraudsters becoming increasingly sophisticated.

New and evolving data privacy regulations also place pressure on retailers to correctly implement new systems and ensure robust protective frameworks are in place, and risks associated with cyber and privacy regulations were cited by 76 percent of retailers. Meanwhile, in this year's CFO survey, nearly 7 in 10 retail CFOs said they expected cyber regulation to grow in 2016. In the past quarter alone, there has been a spotlight cast on regulators' involvement in cybersecurity and conversations around data privacy versus national security, with President Obama's recently unveiled Commission on Enhancing National Cybersecurity and the dispute between Apple and the FBI over unlocking a suspected terrorist's iPhone.

These regulatory bodies are joining efforts with the U.S. credit card industry, which last year called for compliance with Europay, Mastercard and Visa (EMV) standards mandating more sophisticated authentication technology and shifting greater fraud risk to the retailers. By upgrading their card acceptance and processing systems to use chip-enabled credit cards and devices, retailers are arming themselves against the risks associated with credit card fraud. According to this year's CFO survey, most retailers (76 percent) have completed the EMV transition of their payment terminals—a process which can take months and be costly for businesses. The EMV transition has also caused transaction times at EMV-compliant retailers to take longer, delaying checkout lines and causing frustration among merchants and customers alike. In a move to solve this problem, Visa recently launched new chip software, Quick Chip for EMV, that will reduce payment transactions to about two seconds, from the 20 seconds it currently takes for terminals to process chip cards, while still maintaining the same level of security, according to Visa's press release.

"Mandating EMV chip-compliant payment systems is an important first step in shoring up the industry's cyber defenses, but it's just the tip of the iceberg. Online and mobile transactions remain vulnerable to credit card fraud and identity theft, and POS systems can still be hacked and provide an access point to retailers' networks. New forms of malware can also compromise retailers' IT infrastructure and disrupt business operations. Every retailer will experience a data breach at some juncture; the real question is what mechanisms have been put in place to mitigate the impact."

Shahryar Shaghaghi, National Leader of the Technology Advisory Services practice group and Head of International BDO Cybersecurity

Spotlight on Cybersecurity

Target's massive data breach at the end of 2013 is arguably the event that woke up the world to cyber. A sophisticated malware attack on the retailer's POS system enabled the hackers to steal credit card information from more than 70 million shoppers, making it one of the largest retail hacks ever. Shortly thereafter, Home Depot and eBay were breached, to the tune of 53 million and 145 million compromised records respectively.

These headline-making cyberattacks may have shed light on retailers' vulnerability to data breaches, but the industry's response has done little to deter hackers. According to Verizon's 2015 Data Breach Investigations Report, retailers saw an average of 801 malware events per *week* in 2015, the second-highest volume of attacks, surpassed only by the frequency of attacks on educational institutions. And while the majority of retail cyber incidents are the result of point-of-sale intrusions, cybercriminals have expanded their arsenal to include denial of service (DoS) and distributed denial-of-service (DDoS) techniques, among other forms of malware.

What steps can retailers take to avoid becoming the next target? Prevention is only one component of cyber preparedness. Expect to get hit, and know how you'll respond.

Adopt a cybersecurity framework: The Retail Industry Leaders Association has expressed support for industry adoption of the National Institute of Standards and Technology (NIST) Cybersecurity Framework—a risk-based set of industry standards and best practices aimed at reducing and better managing cyber risks. While not a one-size-fits-all solution, the NIST framework provides a basic roadmap for retailers to assess their organization's cyber readiness, identify and prioritize vulnerabilities according to risk tolerance and criticality, and implement activities to support core functions.

Protect the POS system: POS systems remain the most common entry point for cybercriminals. EMV chips offer more sophisticated authentication technology, cutting down on fraudulent credit card transactions. However, retailers need an additional layer of security for the cardholder's information *after* the transaction is in the system. Build IT firewalls that make it possible to isolate the POS system from other systems in the broader business network and monitor for intrusions. Establish clear protocols for handling sensitive payment card data.

Create and run scenario training events: "Tabletop exercises" that walk step-by-step through an incident response plan can uncover planning and response gaps and lead to preventive remediation work. Scenario training events can also include department-level training and drills to practice the plan so that every employee—from the sales assistant to the CEO—understands his or her role, and so the incident response team can gather the insights it needs to apply the learning from one breach to prevent future breaches.

Don't forget third parties. In this era of the extended enterprise, a single data breach can have ramifications across the entire supply chain. For example, a data security incident at Staples forced five other major retailers to shut down their photo processing sites. Before contracting with a new vendor, understand the potential liabilities and make sure their security controls are up to par. Regularly assess cyber risk from your third-party relationships, understand who has network access and set clear responsibilities.

Share information. When it comes to outsmarting cyber criminals, industry-wide collaboration is a must. Consider participating in an information sharing network, such as the Retail Information Sharing & Analysis Center (ISAC), to stay updated on potential threats and actionable intelligence.

Evaluate proactive cyber defense technology solutions. A variety of new technologies, including artificial intelligence, machine learning and probabilistic mathematics, offer more visibility into customer behavior, earlier detection of intrusions and faster response times.

10 Years of 10-K Disclosures

Between 2007 and now, the retail industry weathered a recession, dramatically expanded e-commerce channels and distribution networks, and watched consumer preferences evolve. And as retailers' strategies changed, so too did their key risk factors. With 10 years of data on top risks, our report has become a bellwether of change and a pulse on where boardrooms and C-suites are focused.

Looking Back

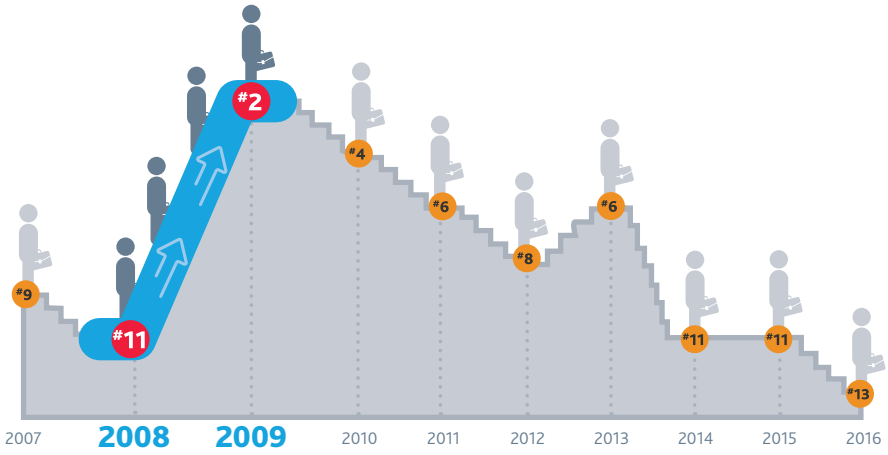
In 2007, impediments to U.S. growth and expansion was the third most-cited risk factor, compared to the 20th most-cited in 2012 and the 10th most-cited this year. Store expansion plans may have been top of mind for retailers in early 2007, but by 2008 and 2009, consumer spending had significantly pulled back. During those years, companies were focused on adjusting their approaches and, in some cases, rethinking their assets and business units. Restructuring and reorganization were cited by one-in-four retailers in 2012 and almost half by 2015.

With resources constrained, concern over access to credit markets and levels of indebtedness skyrocketed from the 11th most cited risk in 2008 to the second in 2009, and has remained in or near the top 10 risk factors across the industry ever since.

Even as consumers pulled back from brick-and-mortar stores, the rise of e-commerce meant that retailers needed to invest heavily in their technology, infrastructure, distribution networks and executive talent to meet demand. Risks associated with implementation of IT and technology systems were cited by just 50 percent of retailers in 2007, compared to more than 9 in 10 over the past three years. Impediments to e-commerce strategy and growth have proliferated as a concern among the nation's largest retailers, noted by 57 percent this year, compared to just 12 percent in 2007. Still, as digital channels exploded, so too did concerns over protecting consumer and business data.

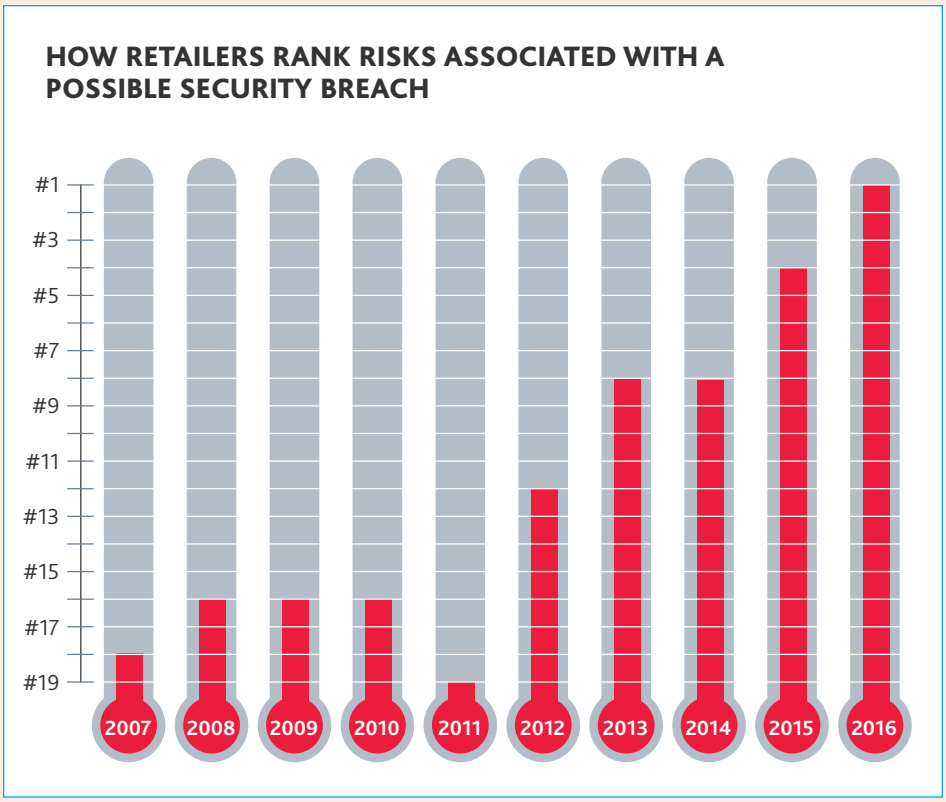
Security concerns were only a blip on retailers' radars in 2007, cited by just 26 percent of companies. But as consumer data breaches grew more prevalent, hackers became more advanced, and vulnerabilities multiplied with new channels and data, prompting concerns over cybersecurity to surge over the next 10 years. Today, they are undeniable and inescapable, with 100 percent of retailers disclosing security concerns in their annual filings.

HOW RETAILERS RANK RISKS ASSOCIATED WITH CREDIT MARKETS/AVAILABILITY OF FINANCING AND COMPANY INDEBTEDNESS



Looking Forward

Nearly every year we add new risk factors to our research, as new challenges arise for the retail industry, and disclosures become more detailed. One area we've been watching closely is the regulatory space. Federal, state and local regulations has been a top 10 risk factor since the beginning of our study, but as landmark legislation like Dodd-Frank and the Affordable Care Act have been implemented, we've seen sentiment change in the retail industry. More recently, a renewed focus abroad and growing enforcement of corruption and bribery laws have sparked greater concern over compliance with the Foreign Corrupt Practices Act (FCPA). Accounting and financial reporting compliance risk also appears to be increasingly prevalent among the nation's largest retailers. Changing practices for both public and private companies, spurred recently by the newly issued standards for revenue recognition and lease accounting, are just beginning to be noted in 10-K filings, but we expect those concerns to rise as retailers prepare and plan for implementation in the coming years.



The Digital Norm Poses Competitive and Growth Risks

Behind the ever-increasing threat of cybersecurity is the new norm of the digital world and payment preferences. E-commerce sales accounted for 7.3 percent of total sales in 2015, and mobile commerce's share of total digital spending is expected to reach 25 percent by the end of this year, according to U.S. Census Bureau data and ComScore. As they look to keep pace with evolving consumer demands and stay afloat in this digital-centric landscape, more than half of leading retailers (57 percent) cite potential impediments to their e-commerce initiatives and changing internet trends as a risk this year. The prevalence of this risk has doubled since 2013, when just 28 percent of retailers cited it as a concern.

While adapting to changing consumer preferences is the bare minimum required to survive, it's not enough to stand out. Competition and consolidation throughout the industry remains a top concern this year, cited by 98 percent of retailers. Recent deal announcements, including DSW's plans to acquire e-tailer Ebuys Inc. and Hudson's Bay Company's acquisition of Gilt Groupe, reflect the growing trend of retailers using an acquisition strategy to boost e-commerce capabilities versus building them from scratch.

Remaining relevant in this hyper-competitive landscape means being strategic as retailers invest in growth and embrace opportunities to deliver speed, convenience and cohesive shopping experiences.

Shoppers have grown to expect expedient product delivery at a low cost, and the battle for the best service is on as brands aim to compete with Amazon's same-day delivery service and startup companies like Deliv. Some retailers are striving to minimize shipping costs and boost delivery speed by transforming stores into mini-distribution centers, or promoting ship-from-store and buy-online-pick-up-in-store programs. Whatever the strategy, postage and shipping fees are becoming a bigger line item on retailers' budgets, and risks associated with postal costs are cited by 17 percent this year, up from 7 percent last year and just 1 percent in 2011. In January, for example, USPS implemented shipping rate increases of 9.5 percent on average, while UPS increased both Air and Ground rates at the end of 2015.

Retailers' abilities to expand their footprints and geographic coverage are also impacted by the accelerated shift from brick-and-mortar to online shopping, which is

evidenced by the uptick in retailers like Wal-Mart, American Eagle and The Gap that are planning to restructure their brick-and-mortar presence. In fact, between January and March of this year, 46 retail chains announced plans to contract their physical stores, according to *About.com*. Recognizing that the full pie of physical stores is shrinking, 90 percent of retailers are concerned about potential impediments to U.S. growth and expansion, up significantly from 56 percent in 2013.

Real Estate Concerns Grow More Prevalent

As retailers consider the impact of the rise of e-commerce on their physical stores, risks related to owning and leasing real estate are cited by more than half of retailers this year (54 percent), a jump from 40 percent last year and 26 percent in 2013.

To make the most of physical space, retailers are investing in redesigning and remodeling their brick-and-mortar stores. For example, retailers, including Forever 21, Old Navy, Staples and Best Buy are moving away from their traditional mega-stores and reducing square footage in existing locations. Meanwhile, Macy's recently announced plans to transform its Los Angeles flagship by expanding its women's apparel, shoes and cosmetics areas and developing higher-profile departments for its luxury brands. But capturing sales by revamping stores will only be effective if retailers can compel shoppers to visit, starting with having an appealing and convenient location—a challenge in itself.

Lease Accounting

The FASB's new lease accounting standard, ASU 2016-02, Leases (Topic 842), was issued on Feb. 25, 2016, and is designed to bring greater transparency on companies' lease assets and liabilities. The new standard, which is effective for fiscal years beginning after Dec. 15, 2018, for public companies, and Dec. 15, 2019 for private companies, including interim periods within those fiscal years, requires:

LESSEES: to record a Right of Use (ROU) asset and a lease liability on the balance sheet for all leases with terms longer than 12 months. Leases will be classified as either finance or operating, with classification affecting the pattern of expense recognition in the income statement. A modified retrospective transition approach is required for lessees for capital and operating leases existing at, or entered into after, the beginning of the earliest comparative period presented in the financial statements, with certain practical expedients available.

LESSORS: to classify leases as either sales-type, finance or operating. A lease will be treated as a sale if it transfers all of the risks and rewards, as well as control of the underlying asset, to the lessee. If risks and rewards are conveyed without the transfer of control, the lease is treated as a financing. If the lessor doesn't convey risks and rewards or control, an operating lease results. A modified retrospective transition approach is required for lessors for sales-type, direct financing, and operating leases existing at, or entered into after, the beginning of the earliest comparative period presented in the financial statements, with certain practical expedients available.

The retail sector will arguably experience the greatest impact of the new lease accounting standard, as they largely rely on leasing for their operations. The lease accounting standard is expected to influence key performance metrics and potentially real estate strategy.

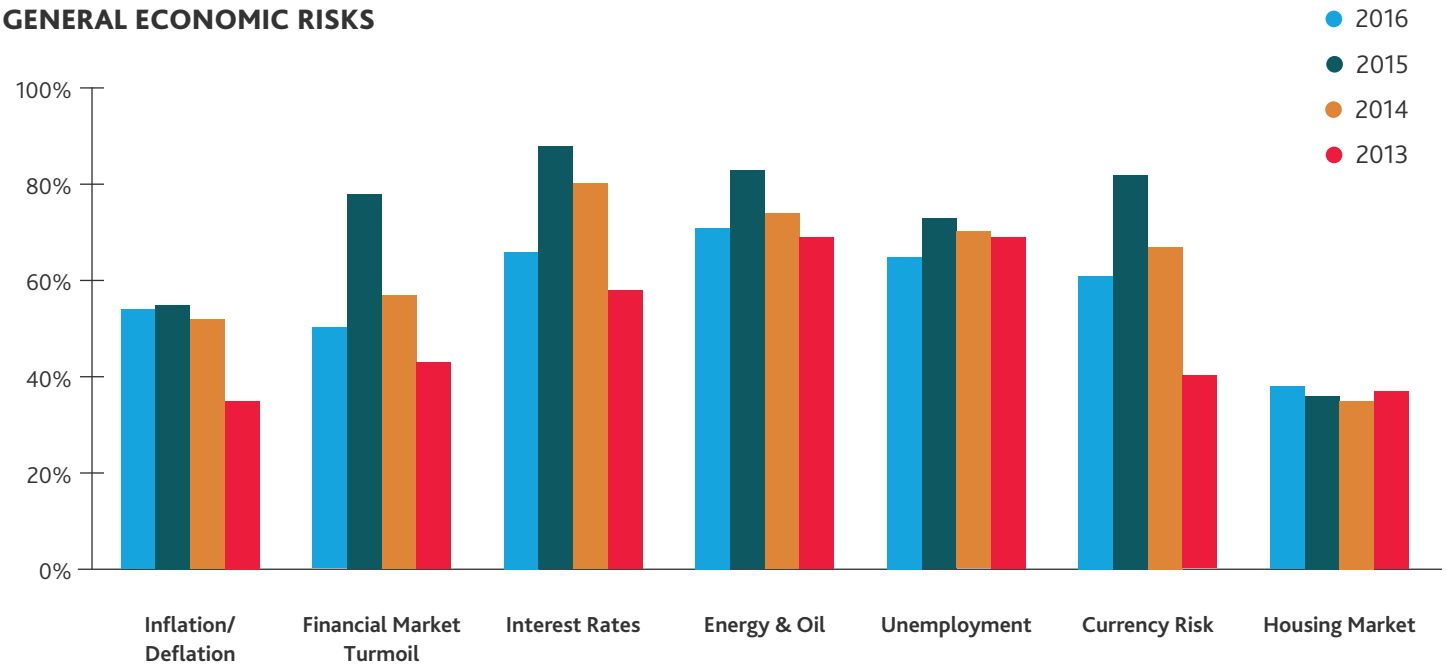
In fact, market competition for prime commercial real estate is cited by nearly half (46 percent) of retailers this year, up from 27 percent last year.

Owning and leasing real estate can present challenges associated with the long-term value of properties and lease negotiations, and now retailers are faced with the FASB's new lease accounting standard. Seventy-six percent of retailers cite accounting standards and compliance as a risk this year, and 14 percent specifically point to lease accounting worries.

"There are three critical things that retailers need to do to prepare for the new lease accounting standard. They need to take the time to fully understand the new rule's impact on their businesses, make sure investors are educated about forthcoming metric and financial reporting changes, and assess the need for shifts in their overall real estate strategies and management systems. It's important for retailers to think about the bigger picture economics of their lease obligations beyond just the accounting."

Stuart Eisenberg, partner and leader of BDO's Real Estate and Construction practice

GENERAL ECONOMIC RISKS



Reading Between the Lines on Economic Concerns

Retailers experienced intense volatility in 2015, marked by energy and materials stocks suffering double-digit drawdowns, the Dow plunging over 1,000 points in August, massive economic disruption driven by conflicts at the West Coast port, the European Central Bank's aggressive monetary stimulus and uncertainty leading up to the Federal Reserve's decision to raise interest rates. And although all 100 retailers continue to see changes in general economic conditions as a potential risk to their businesses, nearly all specific concerns—including energy and oil prices, unemployment rates, interest rates and financial market turmoil—have subsided compared to last year.

Competition & Wage Hikes Drive Labor Concerns

In March of this year, the number of Americans filling out applications for unemployment benefits dropped to the lowest level since November 1973, according to the Labor Department. With more talent in the workforce, labor risks remain top of mind for 91 percent of retailers as they look to hire and retain qualified stores associates and distribution center employees. Positive unemployment trends are also reflected in the number of retailers who expect to boost employee headcount this year, which grew to 48 percent in this year's Retail Compass Survey of CFOs, up from 33 percent in 2015.

While the improving economy and notably low unemployment levels mean that workers feel more freedom to find new jobs, retailers are pushed to think more strategically about how to compensate and incentivize all employees. Driven by competition, some retailers like Wal-Mart and T.J. Maxx announced plans to increase wages as early as last year, but now wage hikes are no longer voluntary in some states. In response to both competitive

"A third of the largest retailers are concerned with enforcement of, and compliance with, anti-corruption and bribery regulation this year, and the stakes have never been higher. We are seeing unprecedented international regulatory coordination and a greater emphasis on individual accountability for corporate misconduct, as articulated by the Yates Memo. The bar for cooperation credit has also been set much higher, with new guidance on self-disclosure and remediation clarifying requirements. The retail industry is far from immune to bribery and other forms of corruption. Retailers should re-evaluate their internal compliance programs and internal investigation protocols to account for the new standards."

Glenn Pomerantz, partner and leader of BDO's Global Forensics practice

motivators and growing regulation, more than one-third (36 percent) of retailers cited concerns over minimum wage increases.

Competition for key leaders also remains fierce, as retailers seek industry veterans with a deep technical understanding of the evolving digital landscape. This year, 73 percent of retailers cite risks related to attracting and retaining key management personnel.

Retailers Remain Cautious about Cross-Border Operations

The global nature of e-commerce, as well as the commodity and materials markets, means that almost every retail business is exposed to international risk. Retailers are well aware of that reality as they look to improve supply chain efficiencies, hedge against currency risks and ensure compliance with international regulations. In addition, the dissolution of the 15-year old Safe Harbor Framework for transatlantic data transfer has raised concerns for online retailers that sell to European consumers and may find themselves in violation of the EU's recently overhauled data protection rules. International operations risks are top of mind for nearly three quarters of retailers (73 percent).

Pricing pressures on commodity prices are specifically cited as a potential risk to almost half (45 percent) of retailers this year. To assuage the anxiety associated with these inflationary pressures on raw materials, retailers are adopting advanced systems to improve supply chain efficiencies throughout their global networks. But since a supply chain disruption can wreak havoc on a retailers' operations, 93 percent still cite concerns about supplier and vendor risks, including shipping and regulatory compliance.

Toyota, for example, recently faced supplier troubles after earthquakes in southern Japan led to a shutdown of 26 car assembly lines, delaying vehicle production and delivery.

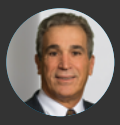
Whether a company has multiple brick-and-mortar stores abroad, broad global e-commerce operations, or is simply pursuing a single cross-border transaction, retailers across the board are tuned in to the potential effects of new and existing international regulations. As U.S. and foreign governments are cracking down on corrupt practices, risks with the FCPA, for example, are cited by one-third (31 percent) of retailers this year.

Technology across all aspects of retailers' operations will only continue to advance, presenting opportunities and challenges related to security and efficiency. The 2016 Retail RiskFactor Report reveals that retailers are well aware of their own exposures that are inherent to technology innovation, from cybersecurity to competition and growth. Looking ahead, retailers need to take the time to assess the risk impact of new technology and related regulation on their channels and target audiences, and ensure that proper controls are in place.

For more information on BDO USA's service offerings to this industry, please contact one of the following regional practice leaders:

DAVID BERLINER
New York
212-885-8347 / dberliner@bdo.com

JENNIFER DI GIOVANNI
Los Angeles
310-557-8274 / jadigiovanni@bdo.com



AL FERRARA
New York
212-885-8000 / aferrara@bdo.com

DOUGLAS HART
San Francisco
415-490-3314 / dhart@bdo.com

NATALIE KOTLYAR
New York
212-885-8035 / nkotlyar@bdo.com

ISSY KOTTON
Los Angeles
310-557-0300 / ikotton@bdo.com

MIKE METZ
Minneapolis
952-656-2612 / mmetz@bdo.com

RICK SCHREIBER
Memphis
901-680-7607 / rschreiber@bdo.com

ALAN SELLITTI
New York
212-885-8599 / asellitti@bdo.com

TED VAUGHAN
Dallas
214-665-0752 / tvaughan@bdo.com

Stay up to date on industry news and trends by following the Consumer Business practice @BDOConsumer or checking out the Consumer Business Compass Blog.

CONTACT US:

FIRST NAME

LAST NAME

EMAIL

PHONE

SUBJECT

MESSAGE

SUBMIT