CYBERHEDGE

Monday
December 9
2019

Cyber Governance Alert

macy's

macy's ★☆☆☆☆

9M	3M	Current
2.22 (▲0.12)	1.66 (▼0.56)	1 (▼0.66)

Cyber-Financial (CyFi) Analysis

- **Strategic KPI for M's business model:** Increased customer loyalty, lower CAC through increased use of technology.
- **How do digital assets create value for M's shareholders?** Customer behavioral data improves personalization / loyalty programs which increases online sales and lowers CAC. 50% of total sales come from M's top 10% of customers.
- **Biggest cyber governance problem:** Evidence of breaches and a lack of people and process to manage the growing risks associated with digital strategy increase the likelihood of a more damaging operational disruption in the next 12-18 months.
- **Biggest financial constraint to fix cyber problems:** Investment in sales and shrinking margins instead of sufficient spend in cybersecurity at a time when it needs to increase cyber governance performance.

Digital transformation plans are key to boosting sales and expanding margins, but poor cyber governance contributes to current underperformance and threatens 12-18-month outlook: Macy's (M), a traditional retailer fighting to stay relevant in an online shopping world, is under enormous competitive pressure to correctly execute its digital transformation plans. The key dilemmas are straightforward. First, in the face of declining sales and shrinking margins, what percentage of its budget should be allocated to technology in order to capture greater market share of both online and traditional retail? Second, what percentage of its IT budget can be spent on protecting those valuable technology investments? So far, likely due to financial constraints, the company has consistently chosen to **underinvest** in adequate protection, resulting in poor performance on cyber governance. The result: losses in shareholder value, underperformance vs. peers and the broader market, reputation (brand value) damage, and disappointing financial results. In addition, M has publicly announced two embarrassing breach events in 2018 and 2019.

Cyberhedge has issued a Cyber Governance Alert on M because we believe the company has little margin for error in executing its digital strategy, and it must allocate the capital necessary **to effectively manage the downside risks of this transformation** to compete with online retail giants. Without better technology risk management, **M is more likely to experience costly business disruption from digital and cyber risks. This would further erode two keystones of the retailer's business in the medium-to-long term: 1) the pricing power that comes from greater market share and 2) more accurate data to forecast customer buying behavior.**

Executing on digital transformation is central to the company's sales growth. Management has been clear about the importance of its digital strategy to current and future growth:

- **Online personalization** is key to marketing its highest-performing products, which drove 37% of total sales in 2018.
- **'Every experience matters'** combines the human touch in M's physical stores with cutting-edge technology in its mobile applications and websites. Key to this point is capturing behavioral data to enhance a customer's experience as they explore stores, mobile applications, and websites.
- **Mobile** is the fastest-growing channel: M delivered more than $1 billion in sales through mobile apps in 2018.
- **Vendor-Direct** now accounts for 10% of online sales. M's 'Amazon play' lets third-party brands fulfill orders and ship directly to customers.

"We curate for our customer through a highly edited assortment that is localized to a specific market, using our enhanced data and analytics, we are able to efficiently influence assortment down to the store level,"

— CEO Jeff Gennette (2018 investor call)

M speaks about its vendor-direct initiative as a connective tissue enabling e-commerce powered by its store network, along with a mobile shopping experience.

This accelerated digital transformation executed under pressure from competitors translates to a vastly expanded and thus more complex IT network. Aggressive IT expansion often comes at the expense of a growing set of new external risks for the company to manage. This, in turn, requires a sufficient investment in security. Currently, the company's spending effort on all aspects of managing digital risks, what we refer to as "cyber governance," is not keeping pace with its ambitious digital growth plans. As this Alert points out, the strains of this underinvestment are already showing.

Potential e-commerce disruption during peak periods should concern investors most.

In recent public comments, management admitted that website difficulties in Q3 were a key contributing factor to the 3.9% drop in sales. M correctly outlines the business disruption risk stemming from a breach in its 10-K, indicating that any failure in its e-commerce platforms could have a material adverse impact on the growth of its business and operating results.

For example, a DDoS attack could disrupt sales during its busiest time of the year and cost the company much more than 3.9%, financial damage that would far surpass a customer data breach in terms of cost and duration. For M's equity and bondholders, this should be added to the list of top business risks requiring attention.

Signs that M management should better allocate the capital necessary to manage its security risks include:

- two public breaches in the past 18 months,
- consistently poor cyber governance scores, and
- the recent indication of how damaging even a minor disruption to e-commerce can be on overall sales.

But should investors be concerned about customer data loss?

Investors should be as concerned about the recent public breach as they appear to be about the Q319 deceleration in sales, but not for the reason many may think. M's share price recovered relative to the overall market after the 2018 breach, and, despite a modest drop following the most recent breach, the share price again wasn't significantly impacted relative to the overall market. However, consecutive breach disclosures serve as additional evidence that M has still not managed to improve its cyber governance. Our data models align with this view. We believe the more recent decline (see chart below) in share price relative to peers is likely reflected in the company's recent downward revision for sales, which, as we point out, is linked to its inability to deliver its e-commerce aims on time. **Taken all together, M's less-than-optimal technology management will be hard to fix as management faces rising risks of: 1) enormous competitive pressure to expand IT and 2) its overall shrinking budget size.**

This is more than a "traditional retailer battling the e-commerce giants" problem:
The below chart shows M's underperformance versus retail peers over the past six months.

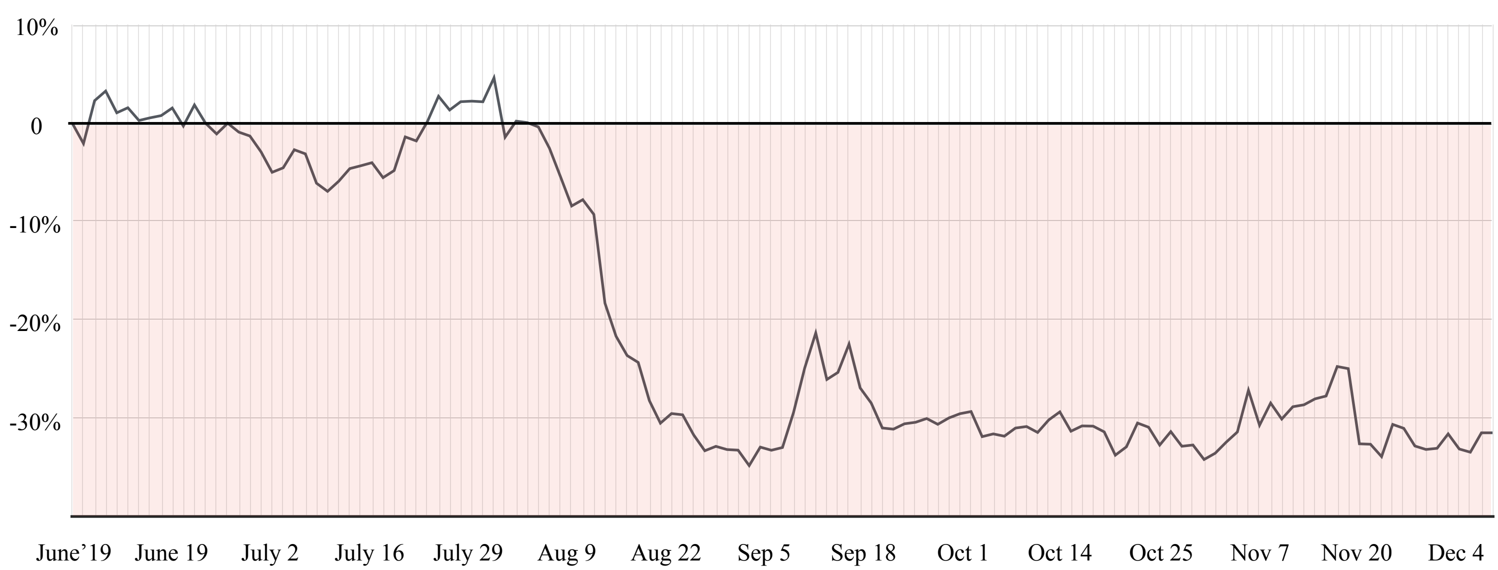

Figure 1. M down 32% vs. peers (S&P Retailers Index) in last six months

Struggling with lower margins also means less $ to allocate to security.

While M's e-commerce strategy has had some success in the past three years, its quarterly online sales growth fell below 10% in the 3Q19 for the first time in a decade, further illustrating the difficult task it faces reviving sales growth. M's strategic priority is to turn around stagnant sales, which requires investment in new marketing approaches ('Backstage') and delivery infrastructure (mobile; e-commerce portal). M also maintains its 489 non-prime store locations in large part due to those locations' value as e-commerce distribution centers (note: in-store sales at these locations are falling faster than in the 150 prime locations, and, despite accounting for 76% of M's store locations, the 489 non-prime stores only account for 50% of in-store sales). **The combination of these pressures mean that M's operating margin has fallen from 10.2% in 2014 to an estimated 5% this year.** This means less cash available to allocate to security improvements to better manage digital risks. Looking ahead, M's most recent cut in sales and net income forecast for 2019 is the second such cut this year. Further, these competitive pressures are unlikely to ease anytime soon, placing significant constraints on 'non-growth' related IT spend now and in the near future.

Bottom Line: M's difficult competitive position and strategic focus on increasing sales means that it is constrained in its ability to sufficiently invest in cybersecurity to manage growing technology risks. Consistently poor cyber governance is contributing to the company's underperformance vs. both peers and the broader market. To combat declining sales* and earnings**, M is investing in both its brick-and-mortar stores and its e-commerce capabities. However, the company faces competitors with large balance sheets and proven success at e-commerce, lending further doubt to whether its core growth strategy will successfully increase sales and net income. With both budgets and capital position shrinking, the company is constrained in its ability to invest outside of its core growth strategy—into necessary risk-management tools, such as cyber governance. In our view, M's continued underinvestment in cybersecurity relative to peers increases the probability of further shareholder value loss. If the next attack results in an operational disruption, such as a DDoS attack, revenue will be hit and the company's two keystones, 1) the pricing power that comes from greater market share and 2) more accurate data to forecast customer buying behavior, will be further eroded. The next 4-6 quarters should reveal if M's management decides to prioritize an increase in security staff and the necessary investments to improve the company's overall cyber governance to peers.

* 3Q19 sales were -3.9% YoY on a comparable basis; 9m19 sales -1.0% YoY on a comparable basis
** 9mo19 Net Income was $224M, down 39% from $368M in 9mo18

Research

Ryan Dodd, Founder and CEO, Cyberhedge
Chris Nolan, Senior Research Analyst, Cyberhedge
Denis Bolshakov, Creative Director, Cyberhedge

Disclaimer