CYBERHEDGE

Cyber Governance Alert

Thursday
November 21st
2019

RITE AID

★☆☆☆☆

	9M	3M	Current
	1.88 (▼0.22)	1.66 (▼0.22)	1 (▼0.66)

Cyber-Financial (CyFi) Analysis

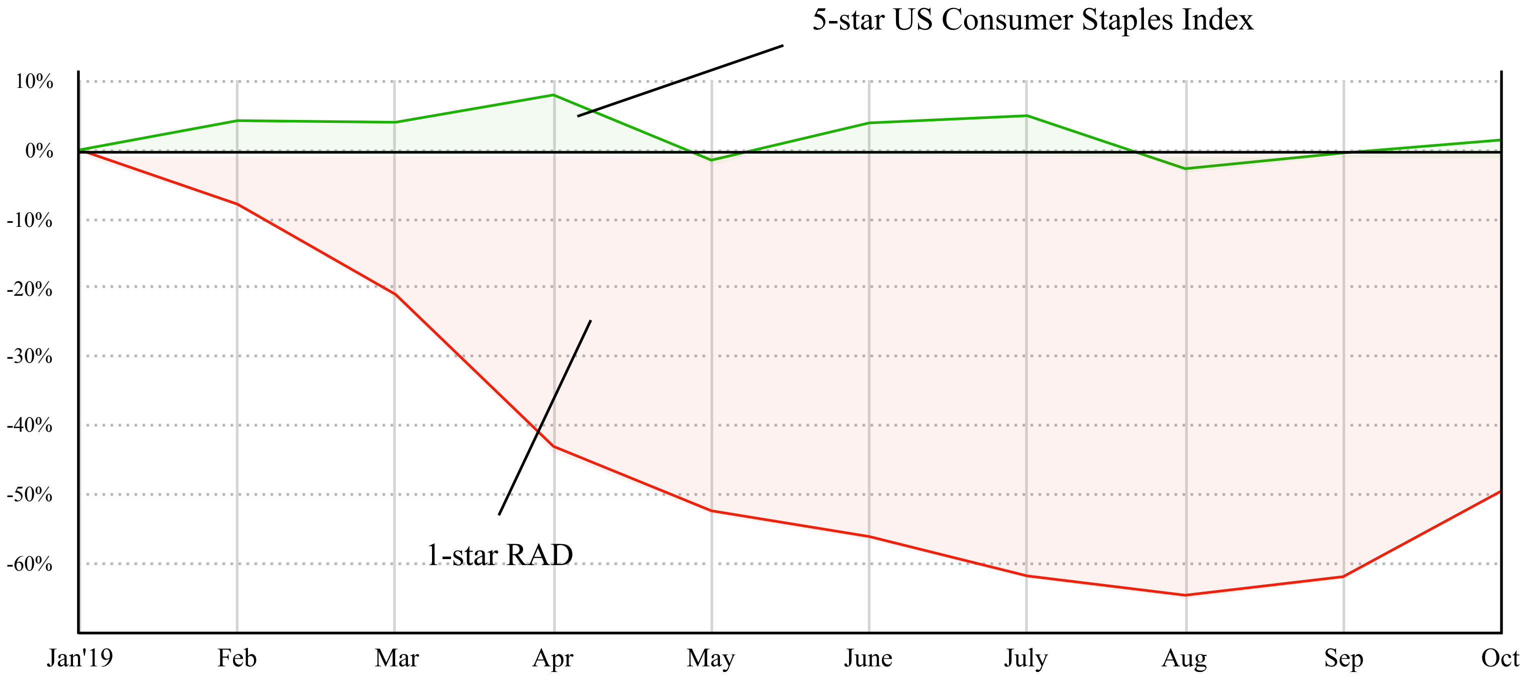
- **Strategic KPI for RAD's business model:** M&A for improved economies of scale.
- **How do digital assets create value for RAD shareholders?** Patient medical data is the highest-value data RAD has to protect—central to the viability of the Rx business that drives the company's revenues and margins.
- **Biggest cyber governance problem:** A complex network with a large threat surface relative to owning a high-value asset for hackers: medical data. Lack of funds required to secure network.
- **Biggest financial constraint to fix cyber problems:** Significant debt load—EBITDA-to-debt ratio increased from 6 to 6.8 in Q2—coupled with declining free cash flow make the necessary security investments more difficult to make.

Structurally Challenged: Rite Aid (RAD) has significant financial constraints and has undergone a management overhaul in an attempt to revive its prospects. It also faces a much greater challenge on cybersecurity relative to other companies because it is both an easy and attractive target for hackers seeking the company's most valuable asset—patient medical data. The new executive team is understandably focused on cost cutting but should not neglect the increased spend required on security in order to better protect this data. Failure to do so could lead to further erosion in RAD's value as a company or attractiveness as an acquisition target.

RAD's 1-star rating is reflective of persistently poor cyber governance that is driven in part by an overly complex corporate IT network (a legacy of M&A and rapid digitization of retail and health care) and an underinvestment in technology security. The problem is that RAD cannot focus on improved growth, cost cutting, and security in the near-term. It can only choose two. Wall St. is pushing for the first two, but we are alerting investors on security, as it could lead to long-term losses.

No secret here: the retail pharmacy is central to RAD's current and future prospects—72% of total EBITDA with profit margins that are 17% higher than the margins on the overall business (Q2 '19). Most of the pharmacy business' value is derived from patient data, which is also the most valuable information to any hacker—10x the value of credit card information by some estimates. A breach of this data damages brand trust/customer loyalty, would cause a costly business disruption in the retail pharmacy business, and would make RAD less attractive to a potential acquirer. All of this at a time when RAD is facing intense competitive pressure from Walgreens and CVS.

Poor cyber governance has already adversely impacted shareholder value.



Companies with poor cyber governance (1-stars) underperform industry peers that perform well (5-stars) and the broader market. Improved cyber governance could play an important role in RAD's recovery.

Bottom Line: Cyberhedge has issued an alert on Rite Aid because the company has little margin for error on cyber-security, especially considering the vital operational and strategic importance of patient medical data to its core retail Rx business. Significant financial constraints—a structural problem, we believe—make it difficult for the company to spend the resources required to fix the underlying problem. Amid the cost cutting, RAD should be careful not to decrease its spend on technology security, but rather increase it in order to better secure its most valuable (for market) and sought-after (for hackers) asset.

CYBERHEDGE

Cyber Governance Alert

Thursday
November 21st
2019

Research

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

Disclaimer