ASA Research Note

WALMART RISK ANALYSIS

AUTHOR: Ananya Mishra

PUBLISHED: January 2024

WRITTEN: October 2022

KEYWORDS: Retail; Cybersecurity; Walmart; Market Expansion;

ABSTRACT: This paper discusses the risk environment of retail giant Walmart within the context of the company's interest in expanding its global reach. However, these expansion efforts will undoubtedly come with increased risks, including regulatory, cybersecurity, operational, and compliance. Looking at both the industry and Walmart's past areas of challenge, the author argues for ways the retailer can mitigate risks in these areas.

It's not news to most people that Walmart Inc. was the world's largest retailer in 2022, measured both by its global revenue and the number of physical retail units. Walmart operates its 4,000 physical stores and a global omni-channel e-commerce platform. As of January 31, 2021, Walmart operated in 25 countries outside the United States (including Canada, China, Japan, United Kingdom, Ghana, Kenya, Nigeria, South Africa, Costa Rica, Guatemala, India, and Mexico).[1] The rate at which the company aims to expand is commendable. In 2022, Walmart—a majority owner of Flipkart with a stake of 72%—announced "that it is considering raising $2 billion to $3 billion at a valuation of more than $40 billion to expand its product range in India and challenge rivals."[2] This demonstrates Walmart's interest in growing its market and gaining access to a more extensive customer base through expansions in several different economies worldwide. However, these expansion efforts will undoubtedly come with increased risks across a variety of areas.

Considerations must include existing laws related to consumer data privacy, financial tax regulations, and strategic relations policies concerning third-party services. Existing laws differ from country to country, and no same rule applies to different countries. For example, suppose Walmart wishes to expand into Europe. In that case, it'll have to comply with the GDPR (General Data Protection Regulation), which has several more layers to consumer data protection than existing laws in the United States.[1] Hence, the levels of risk involved in expanding internationally must be carefully assessed to ensure that every business practice complies with the country's data protection laws and several other policies.

An area of potential control failure concerning Walmart's desire to expand further is its information systems.[3] Walmart is a company that states it relies "extensively on information systems to process transactions, summarize results and manage its business."[4] Given the scale at which Walmart operates through e-commerce, there is a tremendous amount of consumer data to consider regarding data privacy and protection. According to the 10K report, Walmart "also utilize(s) third-party service providers for various reasons, including, without limitation, for digital storage technology, content delivery to customers and members, back-office support, and other functions."[5] Customers place great trust in companies when using

[1] The California Consumer Privacy Act (CCPA) may be the exception to this, as it's primary purpose is to regulate consumer privacy rights

their services, and most of the time, they are not even aware of how their information is being used or how their information is being protected. An example of one of the largest data breaches was one with Target in 2013. Target—which operates at a smaller scale than Walmart—was a victim of a cyberattack by cybercriminals that stole approximately 40 million credit and debit records and 70 million customer records.[6] This demonstrates an imperative need for Walmart to become even more vigilant and take more safety measures to prevent a similar incident.

Walmart's risk factors section of the 10K documentation mentions how the third-party service providers they partner with may have access to information they hold about "customers, members, associates or vendors."[7] Partnering with third-party service providers only increases companies' chances of compromising their consumer's data privacy and invites more cyberattack threats. One way to mitigate this risk is for Walmart to build an in-house security system. This will allow the company to provide better data protection and reduce the platforms and ways Walmart's database can be hacked into. Although this is a massive undertaking for Walmart, it is one of the most efficient ways to prevent such cybercrimes from harming the company. Take Amazon, for example; one of the ways through which Amazon protects its customer's personal information is by having its own security system rather than outsourcing its data for third-party vendors to deal with or uploading it to third-party services' cloud storage. Amazon may share the funding related to customer purchases directly but will not share user data like payment information with third-party service providers, as they make sure not to "sell personal information"[8] to prevent any data breaches from happening.

It is understandable when Walmart says, "Cyber threats are rapidly evolving, and those threats and the means for obtaining access to information in digital and other storage media are becoming increasingly sophisticated."[9] However, for a company as large as Walmart to say: "Some of our systems and third-party service providers' systems have experienced limited security breaches or incidents, and although they did not have a material adverse effect on our operating results, there can be no assurance of a similar result in the future,"[10] is not something an existing or potential customer would be pleased to hear. Their defense to such cases is not having enough information about such cyberattack possibilities before they happen or being unable to deploy enough management resources to prevent any interruptions in their digital operations from running smoothly.[11] However, this indicates that Walmart's leadership fails to understand the gravity of cybercrimes and the danger the company is pushing itself into by not taking enough preventative measures. Hence, another way of mitigating such risks involved in their systems is by making greater use of its resources by hiring more cybersecurity professionals that have in-depth knowledge about ways through which such attacks can be tackled and in-house systems that could be developed (like I mentioned above), as well as having integration between the cybersecurity and research teams. Walmart complains of being unable to keep up with the rapidly evolving cyber threats, which is why the research team should keep updating the cybersecurity team on everything happening in the security field so that the company attempts to remain ahead of cybercriminals.

Another area of weak control is a mix of people and processes.[12] Walmart has had a long history of turning a blind eye to its weak internal accounting controls (dating back to 2003 through 2019).[13] There have been several cases of Walmart's personnel ignoring weaknesses in its internal accounting control, especially in the area of "anti-corruption-related internal controls audit findings."[14] In 2019, Walmart violated the Foreign Corrupt Practices Act (FCPA). Due to this, the company entered into a three-year non-prosecution agreement and agreed to impose compliance monitoring for two years. Walmart also agreed to pay $137 million to settle the U.S. Department of Justice's criminal charges and $144 million to resolve parallel civil

charges brought by the U.S. Securities and Exchange Commission (SEC).[15] Why did Walmart let itself reach a stage of such detriment, where it faced severe fines? Like Charles Cain, Chief of the SEC Enforcement Division's FCPA Unit, rightly said: "Walmart valued international growth and cost-cutting over compliance. The company could have avoided many of these problems, but instead, Walmart repeatedly failed to take red flags seriously and delayed the implementation of appropriate internal accounting controls."[16]

Walmart's leadership displays an eagerness to expand its business in several countries; however, Walmart's choosing to prioritize the speed at which it expands rather than paying more attention to faults in the personnel they decide to be involved in such critical processes is proving to be harmful to the company. The Walmart personnel responsible for maintaining the company's accounting internal control allowed subsidiaries in India, China, Brazil, and Mexico to "employ third-party intermediaries who made payments to foreign government officials without adequate assurances that they complied with the FCPA."[17] These payments were made to expedite and accelerate the process of building/license issuance and access so they could expand the business faster. Walmart delayed the implementation of proper compliance and training when it should've been one of their top priorities. One such case in 2019 was when Walmart discovered findings pointing toward a lack of anti-corruption controls, but "the company continued to retain and renew contracts with third-party intermediaries without conducting the due diligence required by Walmart's internal policies."[18] This is an evident case of weak controls in the company's processes and people.

Although changes have been made since 2019, Walmart should continue to improve its hiring, onboarding, and training processes and implement quarterly employee check-ins to mitigate these risks better. A better hiring process would include following a due diligence checklist for third-party service providers and conducting thorough background checks on employees. The Walmart personnel that failed to "sufficiently investigate or mitigate certain anti-corruption risks" raises the question of the quality of procedures in place and emphasizes the need for improved Walmart employee training that includes the consequences of such unlawful activities. Walmart must strengthen its compliance program to include practices such as onboarding checks that consider past fraudulent activities, relations with foreign nationals, and other information that may be useful in understanding the background of an employee/third-party intermediary. It is also essential for Walmart to have strict quarterly check-ins with their employees to reinforce the training they have received and the third-party relations to ensure that no unusual activity is happening behind the scenes. A more robust tracking system and ensuring that their existing employees are doing the job how it's meant to be done will assist in improving Walmart's reputation and customer trust.

SOURCES

[1] Walmart. (2021, March 19). 10-K (Annual report, Page 8). https://www.sec.gov/. Retrieved October 25, 2022, from https://www.sec.gov/Archives/edgar/data/104169/000010416921000033/wmt-20210131.htm#iaaf0cabf1f7048c9b7e317b3e9c1cfc5_16

[2] Rajesh, A. M. (2022, October 25). Walmart to raise up to $3 billion for Flipkart - mint. Reuters. Retrieved October 25, 2022, from https://www.reuters.com/technology/walmart-raise-up-3-billion-flipkart-mint-2022-10-25/

[3] Searl, Annie. (2022, October). Info 312- Enterprise Risk Management (Fall 2022). Lecture Slides.

[4] Walmart. (2021, March 19). 10-K (Annual report, Page 17). https://www.sec.gov/. Retrieved October 25, 2022, from https://www.sec.gov/Archives/edgar/data/104169/000010416921000033/wmt-20210131.htm#iaaf0cabf1f7048c9b7e317b3e9c1cfc5_16

[5] *Ibid. (Page 18)*

[6] Jones, C. (2022, May 3). Warnings (& lessons) of the 2013 Target Data Breach. Red River | Technology Decisions Aren't Black and White. Think Red. Retrieved October 25, 2022, from https://redriver.com/security/target-data-breach#:~:text=What%20Happened%20During%20the%20Target,was%20one%20of%20the%20largest.

[7] Walmart. (2021, March 19). 10-K (Annual report, Page 17). https://www.sec.gov/. Retrieved October 25, 2022, from https://www.sec.gov/Archives/edgar/data/104169/000010416921000033/wmt-20210131.htm#iaaf0cabf1f7048c9b7e317b3e9c1cfc5_16

[8] Goettsche Partners. (2011). GP. Amazon. Retrieved October 25, 2022, from https://www.amazon.com/gp/help/customer/display.html?nodeId=GX5YKQX9U5LNE63W#:~:text=Information%20about%20our%20customers%20is,examples%20in%20our%20Privacy%20Notice.

[9] Walmart. (2021, March 19). 10-K (Annual report, Page 18). https://www.sec.gov/. Retrieved October 25, 2022, from https://www.sec.gov/Archives/edgar/data/104169/000010416921000033/wmt-20210131.htm#iaaf0cabf1f7048c9b7e317b3e9c1cfc5_16

[10] *Ibid.*

[11] *Ibid. (Page 19)*

[12] Searl, Annie. (2022, October). Info 312- Enterprise Risk Management (Fall 2022). Lecture Slides.

[13] Oh, A., Karp, B., & Mendelsohn, M. (2019, July 16). Walmart's failure to maintain a sufficient anti-corruption compliance program. The Harvard Law School Forum on Corporate Governance. Retrieved October 25, 2022, from https://corpgov.law.harvard.edu/2019/07/16/walmarts-failure-to-maintain-a-sufficient-anti-corruption-compliance-program/

[14] *Ibid.*

[15] *Ibid.*

[16] SEC. (2019, June 20). Press release. SEC Emblem. Retrieved October 25, 2022, from https://www.sec.gov/news/press-release/2019-102

[17] Oh, A., Karp, B., & Mendelsohn, M. (2019, July 16). Walmart's failure to maintain a sufficient anti-corruption compliance program. The Harvard Law School Forum on Corporate Governance. Retrieved October 25, 2022, from https://corpgov.law.harvard.edu/2019/07/16/walmarts-failure-to-maintain-a-sufficient-anti-corruption-compliance-program/

[18] *Ibid.*