UPDATE

Rapid Response

FRIDAY, MARCH 30, 2020

CYBERHEDGE

Marriott

CYBERHEDGE Rapid Response: Marriott

Friday
March 30th
2020

CBH Cyber Governance Rating

1 ★ ☆ ☆ ☆ ☆ (▼6M trend, March 2020)

Example of why transparency on cyber governance is needed

Marriott customer data breach is a continuation of a concerning trend for the world's largest hotel chain, which lacks the financial capacity to fix what is a structural problem, not a one-off incident.

Summary of breach

Marriott International (MAR) reported its second major breach in 2 years, as data on 5.2m loyalty program members was accessed by hackers in January 2020. The hackers gained access to Marriott's IT systems using login credentials of two employees at a hotel property. While the investigation is still ongoing, based on the initial disclosure, it does not appear to be nearly as sizeable as the breach suffered by Marriott in 2018 which resulted in the loss of 400 million customers' data. That breach led to a £99,000,000 (~$123mn USD) fine imposed on Marriott by the United Kingdom's Information Commissioner's Office under the European Union's General Data Protection Regulation (GDPR) (the proceeding is still ongoing).

Continuation of trend of poor cyber governance points to a structural problem

This latest breach is a continuation of a problematic trend for the world's largest hotel chain. Marriott has been an underperformer relative to its hospitality peers on cyber governance (1-Star), and at heightened risk of significant negative financial impact resulting from a breach.

The 2018 breach which stemmed from Starwood's systems inherited in the 2016 acquisition highlighted the material increase in cyber risk following major M&A transactions. This is due in part to the complication of merging two highly complex global IT systems.

These two breaches point to a significant structural problem—the merging of two of the world's largest hotel chains has resulted in an overly complex IT network that is both difficult and expensive to adequately protect. Importantly, Marriott does not currently have the financial capacity to fix it.

This fact runs counter to the perception that this week's news is another one-off incident, in this case a 'minor' customer data breach compared to the 2018 breach.

A technology company with a hospitality business

As we have outlined previously, MAR's business model is often defined by the number of hotels it operates through its vast network of subsidiaries. However, as with most other industries in today's digital age, the true value of the hospitality sector today is not defined by its physical assets. Despite the huge number of hotel buildings in its portfolio, the primary sources of Marriott's value gains are derived from digital assets such as its loyalty cards, reservations systems, the proprietary software underpinning its franchise operations, and other technology designed to drive efficiency and monetize data. The importance of MAR's ability to monetize customer data was evident during the company's Q4 earnings call which outlined the latest loyalty program developments.

And the fact that the customers impacted were loyalty program members is doubly damaging since these are the company's most important and valuable customers.

CYBERHEDGE **Rapid Response: Marriott**

Friday
March 30th
2020

A significant cyber-related disruption could serve as second shock on the heels of the current one

Marriott and other travel-related businesses are of course dealing with an unprecedented operational disruption due to the COVID-19 outbreak, and so this breach comes at a particularly unwelcome time for the company. The financial consequences of a data loss breach of this scale are normally manageable (share price and balance sheet impact), though are still a costly issue to resolve at a time when the company is already significantly cash constrained.

Furthermore, companies such as Marriott will already be dealing with difficulties making the necessary investments to coax customers back into their properties once the current situation around COVID-19 eases.

Coming less than two years after Marriott's 2018 breach, it is clear that the company continues to grapple with an unresolved structural problem that threatens MAR's primary asset, customer data, and further erodes shareholder value.

Due to its underperformance, Marriott currently faces a higher likelihood of a more serious and costly cyber breach that threatens operational disruption such as a ransomware attack on its global reservation systems. Such an event would serve as a secondary shock on the heels of the current COVID-19 disruptions which have resulted in the furloughing of thousands of employees and which could reduce the company's US business by 90 percent until the pandemic passes.

Bottom Line:

MAR management is now dealing with significant financial constraints that make it more difficult to fix a structural problem that threatens the company's primary asset. Management is understandably focused on further cost reductions to weather this unprecedented storm, and likely how to access emergency financing from government economic rescue packages. But MAR should resist reducing investment in cybersecurity at a time when it is already underperforming relative to hospitality peers, as this would increase the probability of shareholder value loss even further.

Management would be prudent to grant the same attention to cyber as it does to other financial risks facing the company. This starts with ensuring it is investing sufficiently in the areas of its security that pose the greatest risk to customer data and digital operations, including its corporate network. Improved cyber governance will increase MAR's ability to take full advantage of the post-COVID-19 economic recovery, and minimize the likelihood of another costly customer data breach or operational disruption.

What do we mean by cyber governance?

Cyberhedge created the performance metric of a cyber governance rating as a way to compare how companies manage their technology investments and network security. The rating is used in the financial industry alongside investment metrics like Return on Equity or Assets (ROE/ROA) or Earnings per share (EPS). We define a corporation's cyber governance as 'the financial impact resulting from how companies manage the operational risks of their technology investments.' Our Cyber Governance Indexes are priced daily and demonstrate market-based proof that better cyber governance does outperform the market and vice versa. For more details, see our CBH ratings.

Research

Ryan Dodd, Founder and CEO, Cyberhedge
Chris Nolan, Senior Research Analyst, Cyberhedge

Disclaimer

The Cyberhedge Research (the “Report”) is not an offer or recommendation to buy or sell or a solicitation of an offer to buy or sell any security or instrument or to participate in any particular trading strategy or be construed as to be a representation or warranty of Cyberhedge (whether express or implied) or its affiliated entities (collectively, the “Cyberhedge Parties” or “Cyberhedge”) regarding the advisability or appropriateness to invest in any security or instrument.

The information and opinions in this report were prepared by Cyberhedge or one of the other Cyberhedge Parties. Though the information herein is believed to be reliable and has been obtained from public sources believed to be reliable, Cyberhedge makes no representation as to its accuracy or completeness. Hyperlinks to third-party websites in the Report are provided for reader convenience only. Cyberhedge neither endorses the content nor is responsible for the accuracy or security controls of these websites.

Further, none of the contents of the Report is intended to constitute investment advice or a recommendation to make (or refrain from making) any kind of investment decision and may not be relied on as such. Reproduction, redistribution or any other form of copying or transmission of the Report without Cyberhedge’s prior written consent is strictly prohibited. Without limiting the generality of the foregoing, the Report and other Cyberhedge intellectual property you access via the Cyberhedge website may not be used as a basis for any financial instruments or products (including, without limitation, passively managed funds and index-linked derivative securities), or used to verify or correct data in any other compilation of data or index, or used to create any other data or index (custom or otherwise), without Cyberhedge's prior written permission.

In no event shall any of Cyberhedge, its affiliates, any of its or their direct or indirect information providers nor any other third-party involved in, or related to, compiling, computing or creating any of the information contained in the Report (collectively, the "Cyberhedge Parties") have any liability to any person or entity for any damages, whether direct, indirect, special, incidental, punitive, consequential (including, without limitation, loss of use, lost profits or revenues or any other economic loss) arising in any manner out of your use or inability to use any of the information or date contained in the Report, even if such party might have anticipated, or was advised or notified of, the possibility of such damages.

You agree to indemnify, defend and hold harmless the Cyberhedge parties from and against any claims, losses, damages, liabilities, costs and expenses, including, without limitation, reasonable attorneys' and experts, fees and costs, as incurred, arising in any manner out of your use of, or inability to use, any information or data contained in the Report.

You acknowledge that (I) the Report and all components thereof constitute copyrighted, database righted, trade secret and/or proprietary information of substantial value to Cyberhedge, (II) that you receive no proprietary rights whatsoever in or to the Report or data or information contained therein, and (III) that title and ownership rights in and to the Report and all the rights therein and legal protections with respect thereto remain exclusively with Cyberhedge. You shall not, and shall not assist any third-party to, assert any rights in the Right or any component thereof or challenge Cyberhedge’s rights therein.

None of the material, nor its content in the Report, nor any copy of it, may be altered in any way, transmitted to, copied or distributed to any other party, without the prior express written permission of Cyberhedge. Cyberhedge will not treat recipients of this report as its customers by virtue of their receiving this report. The legal entities and potential investments in such entities contained or referred to in the Report may not be suitable for you and it is recommended that you consult an independent investment advisor if you are in doubt about such investments or investment services. Nothing in the Report constitutes investment, legal, accounting or tax advice, or a representation that any investment or strategy is suitable or appropriate to your individual circumstances, or otherwise constitutes a personal recommendation to you.

Opinions, estimates and projections constitute the current judgment of the author as of the date of this Report. They do not necessarily reflect the opinions of Cyberhedge and are subject to change without notice. Cyberhedge has no obligation to update, modify or amend the Report or to otherwise notify a recipient thereof if any opinion, forecast or estimate contained herein changes or subsequently becomes inaccurate. Coverage and the frequency of changes in market conditions and in both general and company specific economic prospects makes it difficult to update research at defined intervals. Updates are at the sole discretion of the coverage analyst concerned. The financial instruments discussed in the Report may not be suitable for all investors and investors must make their own informed investment decisions. Prices and availability of financial instruments are subject to change without notice and investment transactions can lead to losses as a result of price fluctuations and other factors. If a financial instrument is denominated in a currency other than an investor's currency, a change in exchange rates may adversely affect the investment. Past performance is not necessarily indicative of future results.

The information we provide is being directed only to persons we believe to be financially sophisticated, who are capable of evaluating investment risks independently, both in general and with regard to particular transactions and investment strategies. If this is not the case, we ask that you inform us immediately.

We and our affiliates, officers, directors, employees, and contractors, excluding equity and credit analysts, will from time to time have long or short positions in, act as principal in, and buy or sell, the securities or derivatives, if any, referred to in the Report.