

Cyber Governance Alert


RYANAIR


12M

6M

Current

2 (▼0.66)

1.8 (▼0.20)

1 (▼0.80)

Cyber-Financial (CyFi) Analysis

- **Strategic KPIs for RYA business model:**

1. Transmission of data and sensors required to ensure efficient operations and market share; 2. Use of behavioral data to improve pricing and routing options that lowers customer acquisition costs and improves operational efficiencies.

- **How do digital assets create value for RYA shareholders?**

The technology platform and use of data and sensors helps RYA improve operational efficiency that helps the low cost airline take market share from competitors. Behavioral data is key to continually improving pricing and route offerings to maintain position as top low cost operator (more people in seats) and growing ancillary sales—an important source of revenue growth.

- **Biggest governance problem:**

An operational disruption to RYA's service stemming from cyber breach, such as a ransomware attack on MyRyanair platform, would hamper the company's operational efficiency at a time it will be looking to take advantage of the post-Covid-19 recovery.

- **What financial metrics investors can track to measure cyber governance:**

Strong short-term liquidity and the ability to access more capital provides the financial capacity to make necessary investments to improve its poor cyber-security in the near term.

Why does Cyber Governance matter?

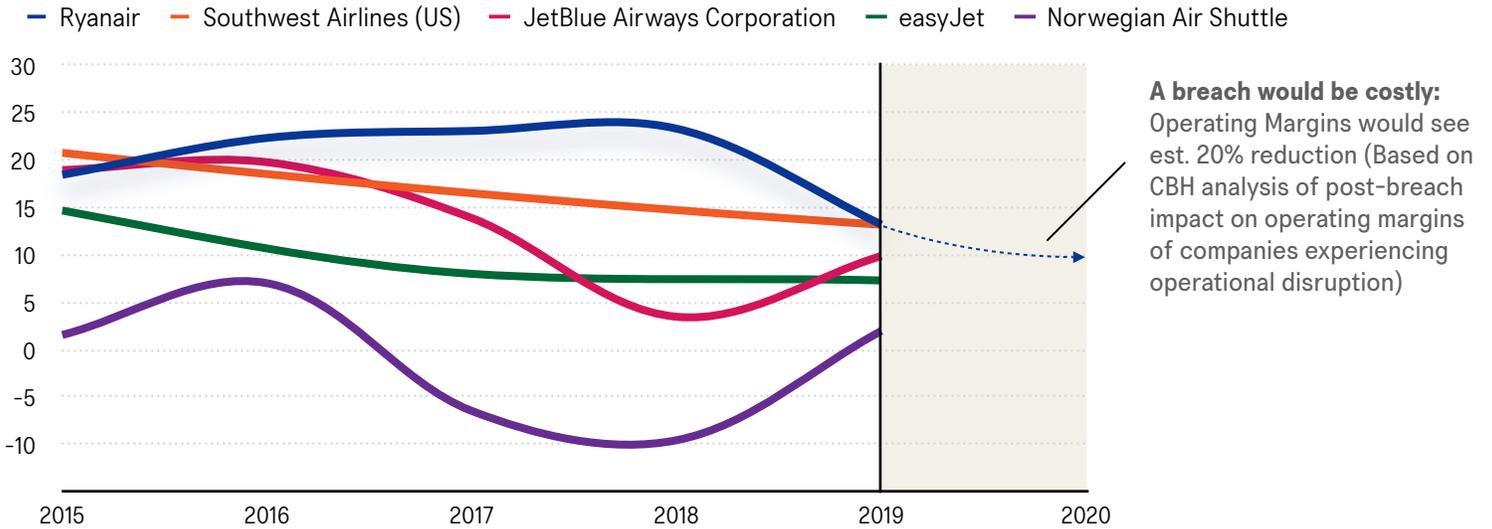
Investors need to know whether management is overinvesting or underinvesting in securing its most valuable asset—technology—relative to the increasing risks the company faces as a result of the ongoing digitization of the business. Ryanair's early and full embrace of digital technology makes cyber an issue that presents significant negative downside financial risk if not properly managed.

Ryanair (RYA) entered 2020 in decent financial shape relative to other low cost airlines. But in addition to the Covid-19 disruption, poor cyber governance (declining 1-Star CBH rating) poses a risk to the company's industry-leading operating margins, the key enabler for RYA's aggressive pricing and thus market share growth post-Covid-19. Importantly, RYA has the financial capacity to make the necessary investments to address key cyber weaknesses in the near term and therefore lower the downside risk of margin declines.

While Ryanair faces significant challenges from the closure of European air travel, the company faces additional challenges from poor cyber governance that threaten the post-Covid-19 recovery. RYA's management understands that technology is key to its current and future success, evident in its stated vision to be a 'digital company that happens to have an airline attached to it'. The company has talked about wanting to be the 'Amazon of the airline industry'.

Technology has played an important role in enabling the company to improve operational efficiencies key to helping RYA gain market share from competitors through aggressive pricing. Going forward, in order to maximize the technology applications needed to maintain its position as the industry's efficiency leader, the company will need strong cyber governance. An operational disruption such as a ransomware attack that hampers the technology platform or booking system would squeeze operating margins and negate a key advantage of the low-cost leader.

Breach would turn RYA's operating margins from industry-leading to middle of the pack



Fortunately, even considering the unprecedented challenges RYA is facing from Covid-19, it has the financial strength relative to peers to make the necessary investments toward improving its cyber governance as all airlines rely more heavily on digital transformation programs.

Questionable cyber governance a problem for 'Amazon of air travel'

RYA's 1-star ranking stems from across-the-board under-performance relative to peers on cyber governance. Based on our proprietary data, weaknesses in the company's cyber relative to peers include the state of the IT network and the people and process that underpin any company's cyber governance. An overly complex IT network like RYA's is both more difficult and more expensive to adequately defend.

RYA's aggressive cost cutting is legendary, but approaching cyber in a similar fashion can lead to flaws that can be much more costly to rectify in the medium-long term. Cyberhedge refers to the Digital Transformation Trilemma, in which companies can choose to invest in 2 out of the 3 of: 1. Top line growth, 2. Cost savings, 3. Security.

It is possible that a corporate culture that has long emphasized low cost has taken steps in the cyber realm that now resulted in a higher likelihood of RYA experiencing an operational disruption that could lead to significant financial loss.

As discussed above, the company understands that the future is in technological initiatives, and its digital push goes back at least as far as the 2016 launch of the MyRyanair platform. These early steps likely increased the degree of complexity in its digital network. The company's strategic decision to grow through M&A is also a negative factor. This has likely put added strain on its corporate network as it does for most acquirers across any sector integrating new systems and people into an already complex network. Companies like Marriott are recent examples of the cyber-financial risks associated with a growth through M&A strategy—one that was a key contributor to the large 2018 customer data breach. The hospitality giant still wrestles with an overly complex global IT network today.

Financial survival and preparing for a post Covid-19 world

During crisis recovery, cyber governance can be a strategic advantage or untimely setback

RYA entered 2020 in decent financial shape relative to other low-cost airlines and is better positioned to survive the Covid-19 disruption to air travel. It has moved quickly to adapt to its current challenges, cutting all staff salaries by 50% for April and May and is communicating to the market that its top priority is to preserve as much cash as possible while operations remain shuttered.

While it is difficult to predict when air travel will resume in Europe (RYA expects operations to be completely shut down in April and May) and at what volume, RYA had over 4 billion Euros of cash and cash equivalents as of March 12. CEO Michael O'Leary projected that the company could survive 12 months of zero revenue. Considering that the company has low leverage (net debt under \$500m) and the ability to access more liquidity (it owns unencumbered aircraft worth \$8B+), RYA has the financial capacity to expand its digital efforts, while making the necessary investments to improve its poor cybersecurity in the near term—even considering the unprecedented challenges facing the airline industry.

It is also worth noting that during the SARS crisis, European airline stock prices fell roughly 40%, and RYA was the best performing of this cohort.

Financial survival and preparing for a post Covid-19 world

In short, the Covid-19 challenges should remind companies that they need to think more about the fragility of their operations. Companies such as RYA that have the financial capacity to allocate more resources to addressing key cyber weaknesses should do so in order to lower the risk of an operational disruption that would undercut a competitive strength-operational efficiency. While there is nothing that RYA's management could have done to prevent Covid-19 from disrupting operations, there is much they can do to lower their financial risk due to how they manage their digital technology moving forward to ensure it remains an industry leader in efficiency.

Bottom Line: Prior to the Covid-19 outbreak, Ryanair was in the best financial position of any European airline, and is well positioned to survive a continued disruption to European air travel and come out of this disruption in an even stronger competitive position. But its poor cyber governance threatens to undermine this position because it poses a heightened risk to otherwise strong operational efficiency. Better cyber governance will put Ryanair on stronger footing to take advantage of a rebound in air travel and reduce the risk of financial and market losses due to a cyber-related operational disruption.

Furthermore, the past month has illustrated how companies with better cyber governance are more resilient in the face of the economic shocks of this pandemic.

Ryanair's early and full embrace of digital technology places it at the core of the company's DNA. Management's decision about whether or not to invest appropriately to resolve key security flaws in the near term is a strategic business decision that will factor into how well the company performs on a relative basis post-Covid-19.

Research**Ryan Dodd**, Founder and CEO, Cyberhedge**Chris Nolan**, Research, Cyberhedge**Kevin Dougherty**, Research, Cyberhedge**Denis Bolshakov**, Creative Director, 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 data 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 Report 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.
