

CYBERHEDGE Rapid Response: Travelex/Finabl

Friday
January 10th
2020

The market's need for external cyber risk ratings. Greater transparency on cyber governance will do more than just tick boxes at the board level. It will help company leadership, equity and bondholders avoid significant market losses.

CBH Cyber Governance Rating	Type of Attack	Operational Impact	Est. Financial Impact	Similar examples
 Dec 2019 ▼ 12M trend	Ransomware / Business Interruption	Lost Revenue, Increase in OpEx, Likely Customer Churn	\$10mn EBITDA over 12M, Potential total post-breach EV loss \$450mn	Maersk, Norsk Hydro, Mondelez, Pitney Bowes

Latest example of why transparency on cyber governance is needed

A cyber risk rating would have mitigated some of the market losses for FIN shareholders since the public learned of the Travelex disruption.

Economic impact

Regarding economic impact, Cyberhedge estimates loss equivalent of 3% of Total EBITDA for 2020 (roughly \$10mn USD based on FY20 estimates). Our estimate would include the minimum viable cost to fix and repair networks as well as lost business. Note that our economic loss estimate **does not include** any damages from lawsuits from retail customers or wholesale partners, a GDPR fine (up to 4% of revenue, est. \$60mn) and any future losses due to customer churn.

Most important are the potential losses to the intangible asset value of the Travelex brand, a leading name in FX.

Weakest Cyber Governance Metric to Peers was key contributing factor

In 2019, the Cyberhedge model consistently measured FIN's weakest cyber governance metric versus peers as a **poorly managed threat surface and technology stack**. In other words, despite being a heavily tech-centric business model, Travelex had not adequately secured what turned out to be relatively easy access into its corporate network due to a vast "threat surface" of entry points including a large global network of Retail PoS, Online Apps and poorly secured network ports.

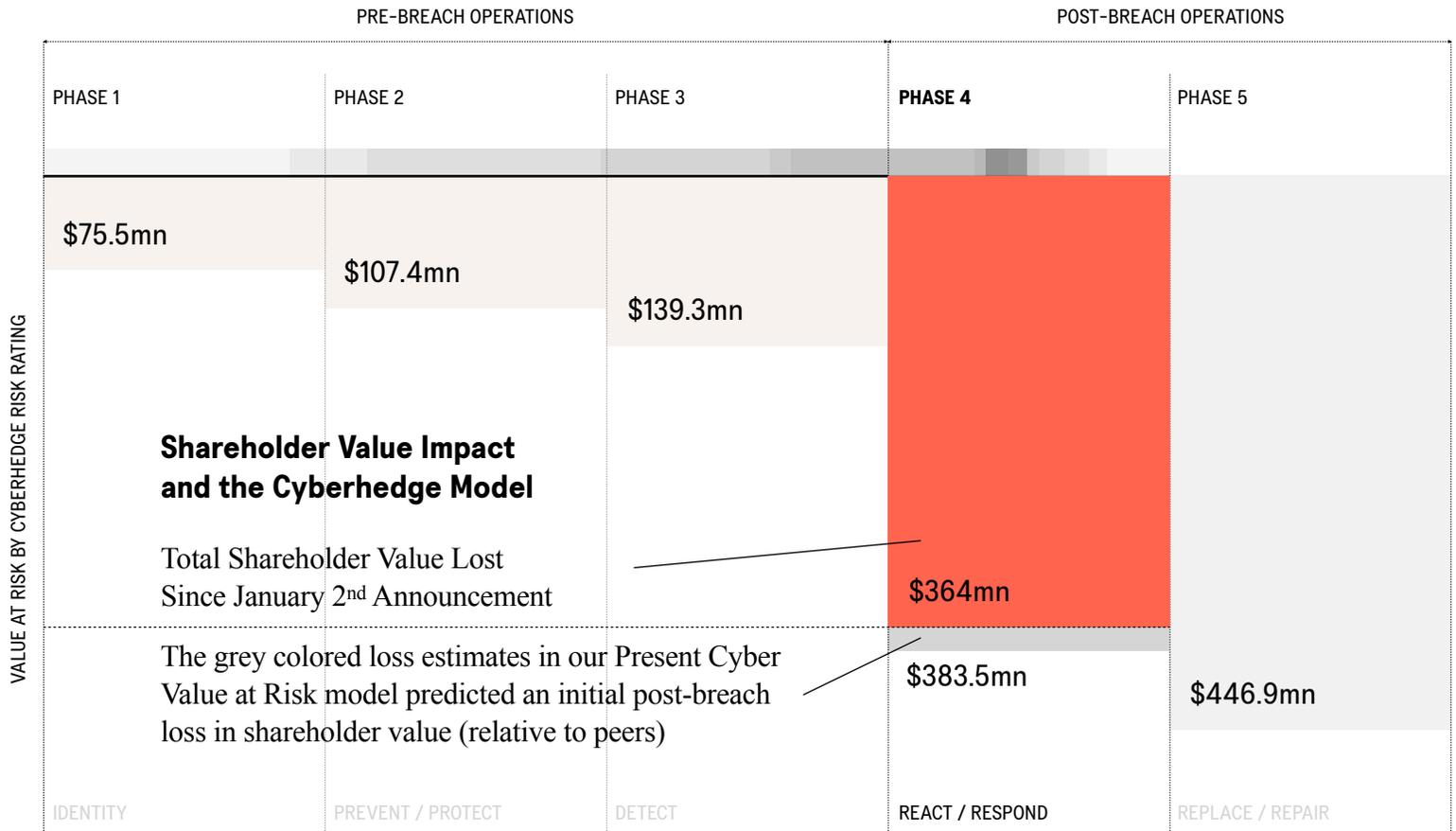
Travelex's weakness appears to have been a key contributing factor to the breach. Based on all available information, the attack vector used (i.e. how the hacker got in) was not sophisticated as they exploited a known vulnerability. The software, however, used to infect the machines **after the hacker got in** was likely complex and difficult to detect, but the "way in" was not. They left the door open (i.e. a known vulnerability left unpatched), and the hackers simply walked in and then deployed their weapons.

CYBERHEDGE Rapid Response: Travelex/Finabl

Friday
January 10th
2020

CBH CVaR model

Pre-breach value (as of Jan 1st, 2020)



Per the above chart, the potential total post-breach shareholder value loss is \$446.9mn or **121p/share** if more information on damages and cost to repair networks are announced.

Why equity and bondholders should be concerned about cyber in near to medium term

Finabl and Travelex have significant financial constraints to improve their cybersecurity in the long-term. The company has **low margins versus peers on operating and net income** (even after the company reports generous “adjustments”). The company also scores below peers on important **debt metrics of EBIT/Int Expense, Interest Coverage and ROA**. This will make the necessary increased investment in cybersecurity more challenging.

CYBERHEDGE Rapid Response: Travelex/Finabl

Friday
January 10th
2020

Two incidents of poor technology management in past two years

Parent company FIN will likely incur unexpected financial losses due to disrupted operations stemming from the attack on Travelex. This event follows a 2018 Travelex breach disclosed in FIN's 2019 prospectus.

Analysis of the breach to date has focused on an unpatched known vulnerability. But vulnerabilities and required patches exist in all corporate networks every day. In this case, what should concern bond and equity holders is that despite a tech-reliant business model, the company was not breached due to a "national security" level sophisticated attack. Rather, it was hit because it mismanaged a basic, fundamental action in good cyber hygiene: patching a vulnerability. The recent oversight is not Travelex's first.

More broadly, **investors should be concerned by the persistence of FIN's poor cyber governance amid rising global ransomware attacks and the operational disruptions that ensue.** In this case, it caused over two weeks of service outages for customers, including at least 14 global banks. Though Travelex management's response has been underwhelming and focused on claims that there is no evidence of customer data loss, **the real issue is that due to business disruption, there is a clear near-term negative financial impact and potentially even bigger future reputation and brand damage** to Travelex's business.

Bottomline: Past underinvestment in security means higher costs and lower cash flows in the near to medium term. Based on Cyberhedge cost estimates from other ransomware attacks at public corporations in recent years (attacks that disrupt business operations, like at Maersk, Norsk Hydro and Pitney Bowes), we believe fixing the problems related to the cyber attack as well as correcting the underinvestment in technology security requires Travelex (and FIN) to spend significantly more money than it has budgeted for. These higher costs could lead to lower-than-expected EBITDA in the coming quarters that will in turn likely further depress the already underperforming share price.

CYBERHEDGE Rapid Response: Travelex/Finabl

Friday
January 10th
2020

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 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.