

● UPDATE

Rapid Response

WEDNESDAY, JUNE 10, 2020

CYBERHEDGE

Honda

CBH Cyber Governance Rating 2 (-0.33) ★★☆☆☆ (▼6M trend, March 2020)

Executive Summary

Honda has been hit with a ransomware attack. Based on the financial impact to corporations hit with similar attacks, it is likely Honda will see a 13-19% incremental decline in operating margin due to increasing security-response costs and technology expenses related to fixing supply-chain disruptions.

Like other 2 Star rated companies, Honda's below average cyber governance (trending lower in the past 6 months) has been warning investors to a potential underperforming share price due to technology challenges the company faces.

Our models show Honda scores worse vs. peers on specific cyber metrics related to **lack of remediation and poor process** in cyber. This suggests a lack of resources and priority to resolve network security problems—**especially due to the warning signs** of Honda's repeated security incidents in the past year.

The severity and duration of the work stoppage is still unknown, but the costs to fix the problems and resume operations will place further financial constraints on company finances already struggling under weight of the pandemic.

BY THE NUMBERS | Honda and Ransomware

Why are successful ransomware attacks increasing?

With many working from home during Covid-19, attackers are taking advantage of WFH employees without protection of their corporate networks.

How is this possible? Poor management of the security stack, i.e. wrong configurations, lack of integration and ineffective monitoring/alerting.

How fast is ransomware increasing?

Increased Rate of Ransomware attacks During Covid-19 (Three Months 4Q 2019 to 1Q 2020)*

↑25%

Worldwide

↑156%

Manufacturing Sector

According to Mandiant/FireEye the Global Leader in Threat Intelligence and Incident Response**:

67%

Attacks are not prevented

74%

Attacks are undetected

91%

Attacks go unreported

According to Forrester survey of Corporate IT Directors about Top IT Security Challenges***

#1 Challenge

IT networks/ environments too complex

#2 Challenge

Evolving Nature of IT threats internally/ externally

What is the Financial Impact?

Notable Ransomware Attacks so far in 2020

EX-POST EVENT	AVG. 3 MONTH MKT VALUE LOSS RELATIVE TO PEERS	ECONOMIC LOSS AS % OF OPER INC
Travelex	-35%	28%
Pitney Bowes	-20%	14%
ISS A/C	-21%	Est. 11-15%, Pending Earnings
Cognizant	-18%	Est. 9-13%, Pending Earnings
Honda	—	Est. 1.5-4%, Pending Earnings

Sources: * Beazley Insurance, Blackfrog Security
 ** Mandiant/FireEye Threat Intelligence Actual data from corporate networks, Mandiant Security Effectiveness Report, May 2020
 *** Forrester Research

Summary of breach

A ransomware attack disrupted Honda's global operations on Monday. This comes at a time when Honda was just getting operations back to capacity after the complete suspension of major facilities spurred by the pandemic. The company is also struggling with a drop in auto and motorcycle sales in every major market in FY20. Honda staff were advised not to access their work computers Monday and to take paid leave on Tuesday, if possible.

Operations spanning Ohio, Honda's main production base in the US, to Turkey, Brazil and Japan were all ground to a halt as the company scrambled to assess the breach that disrupted its network.

Production reportedly resumed at most plants by Tuesday, but its main plant in Ohio, as well as those in Turkey, India and Brazil remain suspended. Honda Customer Service and Honda Financial Services were also taken offline.

This breach comes on the heels of an [August 2019](#) breach when 40GB of company data was discovered on an unsecured database. The data **reportedly included credentials** for some of the company's security systems and networks, technical data on all of its IP addresses, operating systems and code for patches they had used.

Ransomware will further compress operating margins already on downward slide globally

Honda's statement on Tuesday indicated there was no evidence of data loss, but this "data loss" issue **is almost immaterial** compared to the financial impact of an operational disruption for manufacturing plants and supply chains.

Cyberhedge analysis indicates there is an average 13-19% percent drop in operating margins for companies experiencing a cyber-related operational disruption in manufacturing or supply chain due to ransomware. Per Honda's latest earnings call (May 12, 2020) on FY20 results, operating margins of 4.2 percent are already down YOY from '19 (4.6 percent).

Further compression of margins will put further strain on the company's finances at time when sales across all major markets for motorcycles (-4.4%) and autos (-10%) were down in FY20 and likely to be down further still in FY21.

Accelerated digital transformation only complicates challenges for underperformers like Honda

The automobile industry is already years into its digital transformation – from more connected cars to the digitization of the global supply chain, manufacturing processes and customer service. This digitization is evidenced in fact that Honda global operations were halted as a result of a single attack on the corporate network – from cars on the assembly line in Turkey to financing packages for new customers in Brazil.

COVID-19 has accelerated the separation between outperformers and underperformers across all sectors and markets on the basis of good or bad cyber governance. Honda is unfortunately an underperformer that could fall further behind peers that are doing a better job executing on digital transformation.

We would see an improvement of our Cyber Governance rating from 2 to 3 Star, if Honda management can allocate additional resources to addressing underlying weaknesses in the corporate network for a period of 3-6 months.

Bottom Line:

Repeated security incidents in the past year are an indication of significant underlying weaknesses in Honda's cyber governance. Operational disruption will place further financial constraints on margins and company finances already struggling under weight of pandemic. This makes increasing investment in cyber more difficult at a time it is cutting capex in most other areas. But this investment is needed to lower the probability of another significant disruption in future.

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.
