

Statement on Cybersecurity Risks and Mitigation
March 9, 2021

Like most companies today, we face cybersecurity and data protection risks relating to cyber-attacks and information technology failures that could cause loss of confidential information and other business disruptions which could result from individual or highly-coordinated cyber-attacks such as data theft, system breaches, malfeasance or improper use or other unauthorized access to our IT systems. There may also be unintentional technology disruptions, including those resulting from programming errors, employee operational errors and software defects.

Information technology is used and relied upon extensively by our business. We collect, process, and retain sensitive and confidential customer information, including proprietary business information, personal data and other information, some of which may be subject to privacy and security laws, regulations and/or customer-imposed data protection controls. We also provide technological products integral to train operation. Accordingly, we take steps to mitigate these risks and any subsequent adverse impacts to our business these risks may cause.

First, cybersecurity is addressed and discussed at least annually with the Audit Committee and Full Board of Directors. Wabtec also maintains SOC 1 Type 2 certification for select digital products, as well as cyber liability insurance coverage in amounts sufficient for our level of risk. Finally, Wabtec engages in regular security awareness training to highlight and educate its employees on how to identify and mitigate cybersecurity risks at the individual level.

As a result, the Company has not experienced any data or information breaches that caused a disruption of business or any other damages.