Table of Contents

impacting the results of the sensitivity analysis are not matched with the offsetting changes in the values of the items that those instruments are designed to finance or hedge.

The results of the sensitivity analysis at December 31, 2020 and 2019, are as follows:

Interest Rate Risk
A hypothetical 10 percent adverse change in the levels of interest rates with all other variables held constant would result in a decrease in the fair value of our financial instruments of approximately $0.4 billion and $0.6 billion at December 31, 2020 and 2019, respectively. Changes in the relative sensitivity of the fair value of our financial instrument portfolio for these theoretical changes in the level of interest rates are primarily driven by changes in debt maturities, interest rate profile and amount.

Foreign Currency Exchange Rate Risk
A hypothetical 10 percent adverse change in the levels of foreign currency exchange rates relative to the U.S. dollar, with all other variables held constant, would result in a decrease in the fair value of our financial instruments of approximately $1.8 billion and $0.6 billion at December 31, 2020 and 2019, respectively. The increase in the sensitivity of these theoretical changes from the prior year is primarily driven by an increase in Euro denominated long-term debt and a decrease in derivatives used for purchases of foreign currencies.

Financing Risks
See the “Description of Business” on pages 27 to 28 for a discussion of the financing risks associated with the Global Financing business and management’s actions to mitigate such risks.

Cybersecurity
While cybersecurity risk can never be completely eliminated, our approach draws on the depth and breadth of our global capabilities, both in terms of our offerings to clients and our internal approaches to risk management. We offer commercial security solutions that deliver capabilities in areas such as identity and access management, data security, application security, network security and endpoint security. These solutions include pervasive encryption, threat intelligence, analytics, cognitive and artificial intelligence, and forensic capabilities that analyze client security events, yielding insights about attacks, threats, and vulnerabilities facing the client. We also offer professional consulting and technical services solutions for security from assessment and incident response to deployment and resource augmentation. In addition, we offer managed and outsourced security solutions from multiple security operations centers around the world. Finally, security is embedded in a multitude of our products and offerings through secure engineering and operations, and by critical functions (e.g., encryption, access control) in servers, storage, software, services, and other solutions.

From an enterprise perspective, we implement a multi-faceted risk-management approach based on the National Institute of Standards and Technology Cybersecurity Framework to identify and address cybersecurity risks. In addition, we have established policies and procedures that provide the foundation upon which IBM’s infrastructure and data are managed. We regularly assess and adjust our technical controls and methods to identify and mitigate emerging cybersecurity risks. We use a layered approach with overlapping controls to defend against cybersecurity attacks and threats on networks, end-user devices, servers, applications, data and cloud solutions. We draw heavily on our own commercial security solutions and services to mitigate cybersecurity risks. We also have threat intelligence and security monitoring programs, as well as a global incident response process to respond to cybersecurity threats and attacks. In addition, we utilize a combination of online training, educational tools, videos and other awareness initiatives to foster a culture of security awareness and responsibility among our workforce.