Risk Factors Comparison 2023-07-27 to 2022-07-28 Form: 10-K

Legend: **New Text** ~~Removed Text~~ Unchanged Text Moved Text Section

Our operations and financial results are subject to various risks and uncertainties, including those described below, that could adversely affect our business, financial condition, results of operations, cash flows, and the trading price of our common stock. STRATEGIC AND COMPETITIVE RISKS We face intense competition across all markets for our products and services, which may lead to lower revenue or operating margins. Competition in the technology sector Our competitors range in size from diversified global companies with significant research and development resources to small, specialized firms whose narrower product lines may let them be more effective in deploying technical, marketing, and financial resources. Barriers to entry in many of our businesses are low and many of the areas in which we compete evolve rapidly with changing and disruptive technologies, shifting user needs, and frequent introductions of new products and services. Our ability to remain competitive depends on our success in making innovative products, devices, and services that appeal to businesses and consumers. Competition among platform- based ecosystems An important element of our business model has been to create platform- based ecosystems on which many participants can build diverse solutions. A well- established ecosystem creates beneficial network effects among users, application developers, and the platform provider that can accelerate growth. Establishing significant scale in the marketplace is necessary to achieve and maintain attractive margins. We face significant competition from firms that provide competing platforms. • A competing vertically- integrated model, in which a single firm controls the software and hardware elements of a product and related services, has succeeded with some consumer products such as personal computers, tablets, phones, gaming consoles, wearables, and other endpoint devices. Competitors pursuing this model also earn revenue from services integrated with the hardware and software platform, including applications and content sold through their integrated marketplaces. They may also be able to claim security and performance benefits from their vertically integrated offer. We also offer some vertically- integrated hardware and software products and services. To the extent we shift a portion of our business to a vertically integrated model we increase our cost of revenue and reduce our operating margins. • We derive substantial revenue from licenses of Windows operating systems on PCs. We face significant competition from competing platforms developed for new devices and form factors such as smartphones and tablet computers. These devices compete on multiple bases including price and the perceived utility of the device and its platform. Users are increasingly turning to these devices to perform functions that in the past were performed by personal computers. Even if many users view these devices as complementary to a personal computer, the prevalence of these devices may make it more difficult to attract application developers to our PC operating system platforms. Competing with operating systems licensed at low or no cost may decrease our PC operating system margins. Popular products or services offered on competing platforms could increase their competitive strength. In addition, some of our devices compete with products made by our original equipment manufacturer (“ OEM ”) partners, which may affect their commitment to our platform. • Competing platforms have content and application marketplaces with scale and significant installed bases. The variety and utility of content and applications available on a platform are important to device purchasing decisions. Users may incur costs to move data and buy new content and applications when switching platforms. To compete, we must successfully enlist developers to write applications for our platform and ensure that these applications have high quality, security, customer appeal, and value. Efforts to compete with competitors’ content and application marketplaces may increase our cost of revenue and lower our operating margins. Competitors’ rules governing their content and applications marketplaces may restrict our ability to distribute products and services through them in accordance with our technical and business model objectives. PART I Item 1A Business model competition Companies compete with us based on a growing variety of business models. • Even as we transition more of our business to infrastructure-, platform-, and software- as- a- service business model, the license- based proprietary software model generates a substantial portion of our software revenue. We bear the costs of converting original ideas into software products through investments in research and development, offsetting these costs with the revenue received from licensing our products. Many of our competitors also develop and sell software to businesses and consumers under this model. • **We are investing in artificial intelligence (“ AI ”) across the entire company and infusing generative AI capabilities into our consumer and commercial offerings. We expect AI technology and services to be a highly competitive and rapidly evolving market. We will bear significant development and operational costs to build and support the AI capabilities, products, and services necessary to meet the needs of our customers. To compete effectively we must also be responsive to technological change, potential regulatory developments, and public scrutiny. •** Other competitors develop and offer free applications, online services **,** and content, and make money by selling third- party advertising. Advertising revenue funds development of products and services these competitors provide to users at no or little cost, competing directly with our revenue- generating products. • Some companies compete with us by modifying and then distributing open source software at little or no cost to end users, **using open source AI models,** and earning revenue on advertising or integrated products and services. These firms do not bear the full costs of research and development for the open source ~~software~~ **products** . Some open source ~~software~~ **products** ~~mimics~~ - **mimic** the features and functionality of our products. The competitive pressures described above may cause decreased sales volumes, price reductions, and / or increased operating costs, such as for research and development, marketing, and sales incentives. This may lead to lower revenue, gross margins, and operating income. Our increasing focus on cloud- based services presents execution and competitive risks. A growing part of our business involves cloud- based services available across the spectrum of computing devices. Our strategic vision is to compete and grow by building best- in- class platforms and productivity services ~~for~~ **that utilize ubiquitous computing** ~~an~~ **and ambient** ~~intelligent cloud and an intelligent edge infused with artificial~~ intelligence ~~(“ AI~~

~~”)~~ **to drive insights and productivity gains** . At the same time, our competitors are rapidly developing and deploying cloud-based services for consumers and business customers. Pricing and delivery models are evolving. Devices and form factors influence how users access services in the cloud and sometimes the user’ s choice of which cloud- based services to use. **Certain industries and customers have specific requirements for cloud services and may present enhanced risks.** We are devoting significant resources to develop and deploy our cloud- based strategies. The Windows ecosystem must continue to evolve with this changing environment. We embrace cultural and organizational changes to drive accountability and eliminate obstacles to innovation. Our intelligent cloud and intelligent edge ~~worldview is~~ **offerings are** connected ~~with~~ **to** the growth of the Internet of Things (“ IoT ”) **, a network of distributed and interconnected devices employing sensors, data, and computing capabilities, including AI** . Our success in ~~the IoT~~ **driving ubiquitous computing and ambient intelligence** will depend on the level of adoption of our offerings such as Azure, Azure ~~Stack~~ **AI** , **and** Azure IoT Edge ~~, and Azure Sphere~~ . We may not establish market share sufficient to achieve scale necessary to meet our business objectives. Besides software development costs, we are incurring costs to build and maintain infrastructure to support cloud computing services. These costs will reduce the operating margins we have previously achieved. Whether we succeed in cloud- based services depends on our execution in several areas, including: • Continuing to bring to market compelling cloud- based experiences that generate increasing traffic and market share. • Maintaining the utility, compatibility, and performance of our cloud- based services on the growing array of computing devices, including PCs, smartphones, tablets, gaming consoles, and other devices, as well as sensors and other IoT endpoints. • Continuing to enhance the attractiveness of our cloud platforms to third- party developers. • Ensuring our cloud-based services meet the reliability expectations of our customers and maintain the security of their data as well as help them meet their own compliance needs. • Making our suite of cloud- based services platform- agnostic, available on a wide range of devices and ecosystems, including those of our competitors. It is uncertain whether our strategies will attract the users or generate the revenue required to succeed. If we are not effective in executing organizational and technical changes to increase efficiency and accelerate innovation, or if we fail to generate sufficient usage of our new products and services, we may not grow revenue in line with the infrastructure and development investments described above. This may negatively impact gross margins and operating income. **Some users may engage in fraudulent or abusive activities through our cloud- based services. These include unauthorized use of accounts through stolen credentials, use of stolen credit cards or other payment vehicles, failure to pay for services accessed, or other activities that violate our terms of service such as cryptocurrency mining or launching cyberattacks. If our efforts to detect such violations or our actions to control these types of fraud and abuse are not effective, we may experience adverse impacts to our revenue or incur reputational damage.** RISKS RELATING TO THE EVOLUTION OF OUR BUSINESS We make significant investments in products and services that may not achieve expected returns. We will continue to make significant investments in research, development, and marketing for existing products, services, and technologies, including the Windows operating system, Microsoft 365, ~~Office,~~ Bing, SQL Server, Windows Server, Azure, Office 365, Xbox, LinkedIn, and other **products and services. In addition, we are focused on developing new AI platform services and incorporating AI into existing** products and services. We also invest in the development and acquisition of a variety of hardware for productivity, communication, and entertainment **,** including PCs, tablets, gaming devices, and HoloLens. Investments in new technology are speculative. Commercial success depends on many factors, including innovativeness, developer support, and effective distribution and marketing. If customers do not perceive our latest offerings as providing significant new functionality or other value, they may reduce their purchases of new software and hardware products or upgrades, unfavorably affecting revenue. We may not achieve significant revenue from new product, service, and distribution channel investments for several years, if at all. New products and services may not be profitable, and even if they are profitable, operating margins for some new products and businesses will not be as high as the margins we have experienced historically. We may not get engagement in certain features, like **Microsoft** Edge ~~and~~ **,** Bing **, and Bing Chat** , that drive post- sale monetization opportunities. Our data handling practices across our products and services will continue to be under scrutiny ~~and~~ **.** ~~perceptions~~ **Perceptions** of mismanagement, driven by regulatory activity or negative public reaction to our practices or product experiences, could negatively impact product and feature adoption, product design, and product quality. Developing new technologies is complex. It can require long development and testing periods. Significant delays in new releases or significant problems in creating new products or services could adversely affect our revenue. Acquisitions, joint ventures, and strategic alliances may have an adverse effect on our business. We expect to continue making acquisitions and entering into joint ventures and strategic alliances as part of our long- term business strategy. For example, in March 2021 we completed our acquisition of ZeniMax Media Inc. for $ 8. 1 billion, and in March 2022 we completed our acquisition of Nuance Communications, Inc. for $ 18. 8 billion. In January 2022 we announced a definitive agreement to acquire Activision Blizzard, Inc. for $ 68. 7 billion. ~~These~~ **In January 2023 we announced the third phase of our OpenAI strategic partnership.** ~~acquisitions~~ **Acquisitions** and other transactions and arrangements involve significant challenges and risks, including that they do not advance our business strategy, that we get an unsatisfactory return on our investment, that they raise new compliance-related obligations and challenges, that we have difficulty integrating and retaining new employees, business systems, and technology, that they distract management from our other businesses, or that announced transactions may not be completed. If an arrangement fails to adequately anticipate changing circumstances and interests of a party, it may result in early termination or renegotiation of the arrangement. The success of these transactions and arrangements will depend in part on our ability to leverage them to enhance our existing products and services or develop compelling new ones, as well as acquired companies’ ability to meet our policies and processes in areas such as data governance, privacy, and cybersecurity. It may take longer than expected to realize the full benefits from these transactions and arrangements such as increased revenue or enhanced efficiencies, or the benefits may ultimately be smaller than we expected. These events could adversely affect our consolidated financial statements. If our goodwill or amortizable intangible assets become impaired, we may be required to record a significant charge to earnings. We acquire other companies and intangible assets and may not realize all the economic benefit from those acquisitions, which could cause an impairment of goodwill or intangibles. We review our amortizable intangible assets for impairment when events or changes in circumstances indicate the carrying value may not be recoverable. We test goodwill for impairment at least annually. Factors that may be a change in circumstances, indicating that the carrying value of our goodwill or amortizable intangible assets may not be recoverable, include a decline in our stock price and market capitalization, reduced future cash flow estimates, and slower growth rates in industry segments in which we participate. We have in the past recorded, and may in the future be required to record, a significant charge in our consolidated financial statements during the period in which any impairment of our goodwill or amortizable intangible assets is determined, negatively affecting our results of operations. CYBERSECURITY, DATA PRIVACY, AND PLATFORM ABUSE RISKS Cyberattacks and security vulnerabilities could lead to reduced revenue, increased costs, liability claims, or harm to our reputation or competitive position. Security of our information technology Threats to IT security can take a variety of forms. Individual and groups of hackers and sophisticated organizations, including state- sponsored organizations or nation- states, continuously undertake attacks that pose threats to our customers and our IT. These actors may use a wide variety of methods, which may include developing and deploying malicious software or exploiting vulnerabilities **or intentionally designed processes** in hardware, software, or other infrastructure in order to attack our products and services or gain access to our networks and datacenters, using social engineering techniques to induce our employees, users, partners, or customers to disclose passwords or other sensitive information or take other actions to gain access to our data or our users' or customers' data, or acting in a coordinated manner to launch distributed denial of service or other coordinated attacks. Nation- state and state- sponsored actors can deploy significant resources to plan and carry out ~~exploits~~ **attacks** . Nation- state attacks against us ~~or~~ **,** our customers **, or our partners** may intensify during periods of intense diplomatic or armed conflict, such as the ongoing conflict in Ukraine. Inadequate account **security or organizational** security practices may also result in unauthorized access to confidential data. For example, system administrators may fail to timely remove employee account access when no longer appropriate. Employees or third parties may intentionally compromise our or our users' security or systems or reveal confidential information. Malicious actors may employ the IT supply chain to introduce malware through software updates or compromised supplier accounts or hardware. Cyberthreats are constantly evolving and becoming increasingly sophisticated and complex, increasing the difficulty of detecting and successfully defending against them. We may have no current capability to detect certain vulnerabilities **or new attack methods** , which may allow them to persist in the environment over long periods of time. Cyberthreats can have cascading impacts that unfold with increasing speed across our internal networks and systems and those of our partners and customers. Breaches of our facilities, network, or data security could disrupt the security of our systems and business applications, impair our ability to provide services to our customers and protect the privacy of their data, result in product development delays, compromise confidential or technical business information harming our reputation or competitive position, result in theft or misuse of our intellectual property or other assets, subject us to ransomware attacks, require us to allocate more resources to improve technologies or remediate the impacts of attacks, or otherwise adversely affect our business. **We** ~~The cyberattacks uncovered in late 2020 known as " Solorigate " or " Nobelium "~~ are **also subject to** ~~an example of a~~ supply chain ~~attack~~ **cyberattacks** where malware ~~was~~ **can be** introduced to a software provider' s customers, including us, through software updates ~~. The attackers were later able to create false credentials that appeared legitimate to certain customers' systems. We may be targets of further attacks similar to Solorigate / Nobelium as both a supplier and consumer of IT~~ . In addition, our internal IT environment continues to evolve. Often, we are early adopters of new devices and technologies. We embrace new ways of sharing data and communicating internally and with partners and customers using methods such as social networking and other consumer- oriented technologies **. Increasing use of generative AI models in our internal systems may create new attack methods for adversaries** . Our business policies and internal security controls may not keep pace with these changes as new threats emerge, or emerging cybersecurity regulations in jurisdictions worldwide. Security of our products, services, devices, and customers' data The security of our products and services is important in our customers' decisions to purchase or use our products or services across cloud and on- premises environments. Security threats are a significant challenge to companies like us whose business is providing technology products and services to others. Threats to our own IT infrastructure can also affect our customers. Customers using our cloud- based services rely on the security of our infrastructure, including hardware and other elements provided by third parties, to ensure the reliability of our services and the protection of their data. Adversaries tend to focus their efforts on the most popular operating systems, programs, and services, including many of ours, and we expect that to continue. In addition, adversaries can attack our customers' on- premises or cloud environments, sometimes exploiting previously unknown (" zero day ") vulnerabilities, such as occurred in early calendar year 2021 with several of our Exchange Server on- premises products. Vulnerabilities in these or any product can persist even after we have issued security patches if customers have not installed the most recent updates, or if the attackers exploited the vulnerabilities before patching to install additional malware to further compromise customers' systems. Adversaries will continue to attack customers using our cloud services as customers embrace digital transformation. Adversaries that acquire user account information can use that information to compromise our users' accounts, including where accounts share the same attributes such as passwords. Inadequate account security practices may also result in unauthorized access, and user activity may result in ransomware or other malicious software impacting a customer' s use of our products or services. We are increasingly incorporating open source software into our products. There may be vulnerabilities in open source software that may make our products susceptible to cyberattacks. **Additionally, we are actively adding new generative AI features to our services. Because generative AI is a new field, understanding of security risks and protection methods continues to develop; features that rely on generative AI may be susceptible to unanticipated security threats from sophisticated adversaries.** Our customers operate complex IT systems with third- party hardware and software from multiple vendors that may include systems acquired over many years. They expect our products and services to support all these systems and products, including those that no longer incorporate the strongest current security advances or standards. As a result, we may not be able to discontinue support in our services for a product, service, standard, or feature solely because a more secure alternative is available. Failure to utilize the most current security advances and standards can increase our customers' vulnerability to attack. Further, customers of widely varied size and technical sophistication use our technology, and consequently may **still** have limited capabilities and resources to help them adopt and implement state of the art cybersecurity practices and technologies. In addition, we must account for this wide variation of technical sophistication when defining default settings for our products and services, including security default settings, as these settings may limit or otherwise impact other aspects of IT operations and some customers may have limited capability to review and reset these defaults. Cyberattacks ~~such as Solorigate / Nobelium~~ may adversely impact our customers even if our production services are not directly compromised. We are committed to notifying our customers whose systems have been impacted as we become aware and have ~~available~~ **actionable** information ~~and actions~~ for customers to help protect themselves. We are also committed to providing guidance and support on detection, tracking, and remediation. We may not be able to detect the existence or extent of these attacks for all of our customers or have information on how to detect or track an attack, especially where an attack involves on- premises software such as Exchange Server where we may have no or limited visibility into our customers' computing environments. Development and deployment of defensive measures To defend against security threats to our internal IT systems, our cloud- based services, and our customers' systems, we must continuously engineer more secure products and services, enhance security **, threat detection,** and reliability features, improve the deployment of software updates to address security vulnerabilities in our own products as well as those provided by others, develop mitigation technologies that help to secure customers from attacks even when software updates are not deployed, maintain the digital security infrastructure that protects the integrity of our network, products, and services, and provide security tools such as firewalls, anti- virus software, and advanced security and information about the need to deploy security measures and the impact of doing so. Customers in certain industries such as financial services, health care, and government may have enhanced or specialized requirements to which we must engineer our products and services. The cost of measures to protect products and customer- facing services could reduce our operating margins. If we fail to do these things well, actual or perceived security vulnerabilities in our products and services, data corruption issues, or reduced performance could harm our reputation and lead customers to reduce or delay future purchases of products or subscriptions to services, or to use competing products or services. Customers may also spend more on protecting their existing computer systems from attack, which could delay adoption of additional products or services. Customers, and third parties granted access to their systems, may fail to update their systems, continue to run software or operating systems we no longer support, or may fail timely to install or enable security patches, or may otherwise fail to adopt adequate security practices. Any of these could adversely affect our reputation and revenue. Actual or perceived vulnerabilities may lead to claims against us. Our license agreements typically contain provisions that eliminate or limit our exposure to liability, but there is no assurance these provisions will withstand legal challenges. At times, to achieve commercial objectives, we may enter into agreements with larger liability exposure to customers. Our products operate in conjunction with and are dependent on products and components across a broad ecosystem of third parties. If there is a security vulnerability in one of these components, and if there is a security exploit targeting it, we could face increased costs, liability claims, reduced revenue, or harm to our reputation or competitive position. Disclosure and misuse of personal data could result in liability and harm our reputation. As we continue to grow the number, breadth, and scale of our cloud- based offerings, we store and process increasingly large amounts of personal data of our customers and users. The continued occurrence of high- profile data breaches provides evidence of an external environment increasingly hostile to information security. Despite our efforts to improve the security controls across our business groups and geographies, it is possible our security controls over personal data, our training of employees and third parties on data security, and other practices we follow may not prevent the improper disclosure or misuse of customer or user data we or our vendors store and manage. In addition, third parties who have limited access to our customer or user data may use this data in unauthorized ways. Improper disclosure or misuse could harm our reputation, lead to legal exposure to customers or users, or subject us to liability under laws that protect personal data, resulting in increased costs or loss of revenue. Our software products and services also enable our customers and users to store and process personal data on- premises or, increasingly, in a cloud- based environment we host. Government authorities can sometimes require us to produce customer or user data in response to valid legal orders. In the U. S. and elsewhere, we advocate for transparency concerning these requests and appropriate limitations on government authority to compel disclosure. Despite our efforts to protect customer and user data, perceptions that the collection, use, and retention of personal information is not satisfactorily protected could inhibit sales of our products or services and could limit adoption of our cloud- based solutions by consumers, businesses, and government entities. Additional security measures we may take to address customer or user concerns, or constraints on our flexibility to determine where and how to operate datacenters in response to customer or user expectations or governmental rules or actions, may cause higher operating expenses or hinder growth of our products and services. We may not be able to protect information in our products and services from use by others. LinkedIn and other Microsoft products and services contain valuable information and content protected by contractual restrictions or technical measures. In certain cases, we have made commitments to our members and users to limit access to or use of this information. Changes in the law or interpretations of the law may weaken our ability to prevent third parties from scraping or gathering information or content through use of bots or other measures and using it for their own benefit, thus diminishing the value of our products and services. Abuse of our platforms may harm our reputation or user engagement. Advertising, professional, marketplace, and gaming platform abuses For platform products and services that provide content or host ads that come from or can be influenced by third parties, including GitHub, LinkedIn, Microsoft Advertising, Microsoft News, Microsoft Store, Bing, and Xbox, our reputation or user engagement may be negatively affected by activity that is hostile or inappropriate. This activity may come from users impersonating other people or organizations **including through the use of AI technologies** , dissemination of information that may be viewed as misleading or intended to manipulate the opinions of our users, or the use of our products or services that violates our terms of service or otherwise for objectionable or illegal ends. Preventing or responding to these actions may require us to make substantial investments in people and technology and these investments may not be successful, adversely affecting our business and consolidated financial statements. Other digital safety abuses Our hosted consumer services as well as our enterprise services may be used to **generate or** disseminate harmful or illegal content in violation of our terms or applicable law. We may not proactively discover such content due to scale, the limitations of existing technologies, and conflicting legal frameworks. When discovered by users **and others** , such content may negatively affect our reputation, our brands, and user engagement. Regulations and other initiatives to make platforms responsible for preventing or eliminating harmful content online have been enacted, and we expect this to continue. We may be subject to enhanced regulatory oversight, civil or criminal liability, or reputational damage if we fail to comply with content moderation regulations, adversely affecting our business and consolidated financial statements. The development of the IoT presents security, privacy, and execution risks. To support the growth of the intelligent cloud and the intelligent edge, we are developing products, services, and technologies to power the IoT ~~, a network of distributed and interconnected devices employing sensors, data, and computing capabilities including AI~~ . The IoT' s great potential also carries substantial risks. IoT products and services may contain defects in design, manufacture, or operation that make them insecure or ineffective for their intended purposes. An IoT solution has multiple layers of hardware, sensors, processors, software, and firmware, several of which we may not develop or control. Each layer, including the weakest layer, can impact the security of the whole system. Many IoT devices have limited interfaces and ability to be updated or patched. IoT solutions may collect large amounts of data, and our handling of IoT data may not satisfy customers or regulatory requirements. IoT scenarios may increasingly affect personal health and safety. If IoT solutions that include our technologies do not work as intended, violate the law, or harm individuals or businesses, we may be subject to legal claims or enforcement actions. These risks, if realized, may increase our costs, damage our reputation or brands, or negatively impact our revenues or margins. Issues in the development and use of AI may result in reputational **or competitive** harm or liability. We are building AI into many of our offerings, including our productivity services, and we are also making ~~first- and third- party~~ AI available for our customers to use in solutions that they build **. This AI may be developed by Microsoft or others, including our strategic partner, OpenAI** . We expect these elements of our business to grow. We envision a future in which AI operating in our devices, applications, and the cloud helps our customers be more productive in their work and personal lives. As with many innovations, AI presents risks and challenges that could affect its adoption, and therefore our business. AI algorithms **or training methodologies** may be flawed. Datasets may be **overbroad,** insufficient **,** or contain biased information **. Content generated by AI systems may be offensive, illegal, or otherwise harmful** . Ineffective or inadequate AI development or deployment practices by Microsoft or others could result in incidents that impair the acceptance of AI solutions or cause harm to individuals **, customers,** or society **, or result in our products and services not working as intended** . **Human review of certain outputs may be required. As a result of** ~~These~~ **these** ~~deficiencies~~ and other ~~failures~~ **challenges associated with innovative technologies, our implementation** of AI systems could subject us to competitive harm, regulatory action, legal liability, including under new proposed legislation regulating AI in jurisdictions such as the European Union (" EU "), **new applications of existing data protection, privacy, intellectual property, and other laws,** and brand or reputational harm. Some AI scenarios present ethical issues **or may have broad impacts on society** . If we enable or offer AI solutions that **have unintended consequences, unintended usage or customization by our customers and partners, or** are controversial because of their impact on human rights, privacy, employment, or other social, economic, or political issues, we may experience brand or reputational harm **, adversely affecting our business and consolidated financial statements** . OPERATIONAL RISKS We may have excessive outages, data losses, and disruptions of our online services if we fail to maintain an adequate operations infrastructure. Our increasing user traffic, growth in services, and the complexity of our products and services demand more computing power. We spend substantial amounts to build, purchase, or lease datacenters and equipment and to upgrade our technology and network infrastructure to handle more traffic on our websites and in our datacenters. Our datacenters depend on **the availability of permitted and buildable land,** predictable energy ~~and~~ **,** networking supplies, **and servers, including graphics processing units (" GPUs ") and** ~~the~~ **other components. The** cost or availability of ~~which~~ **these dependencies** could be adversely affected by a variety of factors, including the transition to a clean energy economy **, local and regional environmental regulations,** and geopolitical disruptions. These demands continue to increase as we introduce new products and services and support the growth **and the augmentation** of existing services such as Bing, Azure, Microsoft Account services, Microsoft 365, Microsoft Teams, Dynamics 365, OneDrive, SharePoint Online, Skype, Xbox, and Outlook. com **through the incorporation of AI features and / or functionality** . We are rapidly growing our business of providing a platform and back- end hosting for services provided by third parties to their end users. Maintaining, securing, and expanding this infrastructure is expensive and complex, and requires development of principles for datacenter builds in geographies with higher safety **and reliability** risks. It requires that we maintain an Internet connectivity infrastructure and storage and compute capacity that is robust and reliable within competitive and regulatory constraints that continue to evolve. Inefficiencies or operational failures, including temporary or permanent loss of customer data, insufficient Internet connectivity **, insufficient or unavailable power supply** , or inadequate storage and compute capacity, could diminish the quality of our products, services, and user experience resulting in contractual liability, claims by customers and other third parties, regulatory actions, damage to our reputation, and loss of current and potential users, subscribers, and advertisers, each of which may adversely impact our consolidated financial statements. We may experience quality or supply problems. Our hardware products such as Xbox consoles, Surface devices, and other devices we design and market are highly complex and can have defects in design, manufacture, or associated software. We could incur significant expenses, lost revenue, and reputational harm as a result of recalls, safety alerts, or product liability claims if we fail to prevent, detect, or address such issues through design, testing, or warranty repairs. Our software products and services also may experience quality or reliability problems. The highly sophisticated software we develop may contain bugs and other defects that interfere with their intended operation. Our customers increasingly rely on us for critical business functions and multiple workloads. Many of our products and services are interdependent with one another. Each of these circumstances potentially magnifies the impact of quality or reliability issues. Any defects we do not detect and fix in pre- release testing could cause reduced sales and revenue, damage to our reputation, repair or remediation costs, delays in the release of new products or versions, or legal liability. Although our license agreements typically contain provisions that eliminate or limit our exposure to liability, there is no assurance these provisions will withstand legal challenge. There are limited suppliers for certain device and datacenter components. Our competitors use some of the same suppliers and their demand for hardware components can affect the capacity available to us. If components are delayed or become unavailable, whether because of supplier capacity constraint, industry shortages, legal or regulatory changes that restrict supply sources, or other reasons, we may not obtain timely replacement supplies, resulting in reduced sales or inadequate datacenter capacity **to support the delivery and continued development of our products and services** . Component shortages, excess or obsolete inventory, or price reductions resulting in inventory adjustments may increase our cost of revenue. Xbox consoles, Surface devices, datacenter servers, and other hardware are assembled in Asia and other geographies that may be subject to disruptions in the supply chain, resulting in shortages that would affect our revenue and operating margins. LEGAL, REGULATORY, AND LITIGATION RISKS Government litigation and regulatory activity relating to competition rules may limit how we design and market our products. ~~As a leading global software and device maker, government~~ **Government** agencies closely scrutinize us under U. S. and foreign competition laws. Governments are actively enforcing competition laws and regulations, and this includes scrutiny in potentially large markets such as the EU, the U. S., and China. Some jurisdictions also allow competitors or consumers to assert claims of anti- competitive conduct. U. S. federal and state antitrust authorities have previously brought enforcement actions and continue to scrutinize our business. ~~The~~ **For example, the** European Commission (" the Commission ") closely scrutinizes the design of high- volume Microsoft products and the terms on which we make certain technologies used in these products, such as file formats, programming interfaces, and protocols, available to other companies. Flagship product releases such as Windows can receive significant scrutiny under **EU or other** competition laws ~~. For example, in 2004, the Commission ordered us to create new versions of our Windows operating system that do not include certain multimedia technologies and to provide our competitors with specifications for how to implement certain proprietary Windows communications protocols in their own products. In 2009, the Commission accepted a set of commitments we offered to address the Commission' s concerns relating to competition in web browsing software, including an undertaking to address Commission concerns relating to interoperability. The web browsing commitments expired in 2014. The remaining obligations may limit our ability to innovate in Windows or other products in the future, diminish the developer appeal of the Windows platform, and increase our product development costs. The availability of licenses related to protocols and file formats may enable competitors to develop software products that better mimic the functionality of our products, which could hamper sales of our products~~ . Our portfolio of first- party devices continues to grow; at the same time our OEM partners offer a large variety of devices for our platforms. As a result, increasingly we both cooperate and compete with our OEM partners, creating a risk that we fail to do so in compliance with competition rules. Regulatory scrutiny in this area may increase. Certain foreign governments, particularly in China and other countries in Asia, have advanced arguments under their competition laws that exert downward pressure on royalties for our intellectual property. ~~Government~~ **Competition law** regulatory actions and court decisions ~~such as these~~ may result in fines or hinder our ability to provide the benefits of our software to consumers and businesses, reducing the attractiveness of our products and the revenue that comes from them. New competition law actions could be initiated, potentially using previous actions as precedent. The outcome of such actions, or steps taken to avoid them, could adversely affect us in a variety of ways, including **causing us** ~~: • We may have~~ to ~~choose between withdrawing~~ --- **withdraw** products from **or modify products for** certain ~~geographies to avoid fines~~ **markets, decreasing the value of** ~~or~~ **our** ~~designing and developing alternative versions of those~~ **assets, adversely affecting our ability to monetize our** products ~~to comply with government rulings~~ , ~~which may entail a delay in a product release and removing functionality that customers want or on which developers rely. • We may be required to make available licenses to our~~ - **or inhibiting** ~~proprietary technologies on terms that do not reflect their fair market value or~~ **our** ~~do not protect our associated intellectual property. • We are subject to a variety of ongoing commitments because of court or administrative orders, consent decrees, or other voluntary actions we have taken. If we fail to comply with these commitments, we may incur litigation costs and be subject to substantial fines or other remedial actions. • Our~~ ability to ~~realize anticipated Windows post- sale monetization opportunities may be limited. • Regulatory scrutiny may inhibit our ability to~~ consummate ~~acquisitions~~ - **acquisition** or impose conditions **on acquisitions** that **may** reduce ~~the~~ **their** ~~ultimate~~ value ~~of such transactions~~ . **Laws and regulations relating** ~~Our global operations subject us~~ to ~~potential consequences under~~ anti- corruption ~~,~~ **and** trade **could result in increased costs** , ~~and other laws and regulations~~ **fines, criminal penalties, or reputational damage** . The Foreign Corrupt Practices Act (" FCPA ") and other anti- corruption laws and regulations (" Anti- Corruption Laws ") prohibit corrupt payments by our employees, vendors, or agents, and the accounting provisions of the FCPA require us to maintain accurate books and records and adequate internal controls. From time to time, we receive inquiries from authorities in the U. S. and elsewhere which may be based on reports from employees and others about our business activities outside the U. S. and our compliance with Anti- Corruption Laws. Periodically, we receive such reports directly and investigate them, and also cooperate with investigations by U. S. and foreign law enforcement authorities. An example of increasing international regulatory complexity is the EU Whistleblower Directive, initiated in 2021, which may present compliance challenges to the extent it is implemented in different forms by EU member states. Most countries in which we operate also have competition laws that prohibit competitors from colluding or otherwise attempting to reduce competition between themselves. While we devote substantial resources to our U. S. and international compliance programs and have implemented policies, training, and internal controls designed to reduce the risk of corrupt payments and collusive activity, our employees, vendors, or agents may violate our policies. Our failure to comply with Anti- Corruption Laws or competition laws could result in significant fines and penalties, criminal sanctions against us, our officers, or our employees, prohibitions on the conduct of our business, and damage to our reputation. Increasing trade laws, policies, sanctions, and other regulatory requirements also affect our operations in and outside the U. S. relating to trade and investment. Economic sanctions in the U. S., the EU, and other countries prohibit most business with restricted entities or countries ~~such as Crimea, Cuba, Iran, North Korea, and Syria~~ . U. S. export controls restrict Microsoft from offering many of its products and services to, or making investments in, certain entities in specified countries. U. S. import controls restrict us from integrating certain information and communication technologies into our supply chain and allow for government review of transactions involving information and communications technology from countries determined to be foreign adversaries **. Supply chain regulations may impact the availability of goods or result in additional regulatory scrutiny** . Periods of intense diplomatic or armed conflict, such as the ongoing conflict in Ukraine, may result in (1) new and rapidly evolving sanctions and trade restrictions, which may impair trade with sanctioned individuals and countries, and (2) negative impacts to regional trade ecosystems among our customers, partners, and us. Non- compliance with sanctions as well as general ecosystem disruptions could result in reputational harm, operational delays, monetary fines, loss of revenues, increased costs, loss of export privileges, or criminal sanctions. Other regulatory areas that may apply to...... or face regulatory or legal actions. Laws and regulations relating to the handling of personal data may impede the adoption of our services or result in increased costs, legal claims, fines against us, or reputational damage. The growth of our Internet- and cloud- based services internationally relies increasingly on the movement of data across national boundaries. Legal requirements relating to the collection, storage, handling, and transfer of personal data continue to evolve. For example, **while** ~~in July 2020 the Court of Justice of~~ the EU ~~invalidated a framework called~~ **- U. S. Data** Privacy ~~Shield for companies~~ **Framework (" DPF ") has been recognized as adequate under EU law** to **allow** ~~transfer~~ **transfers of personal** data from **the** EU ~~member states~~ to **certified companies in** the **U** ~~United States~~ . ~~This ruling continues~~ **S., the DPF is subject** to ~~generate uncertainty about~~ **further legal challenge which could cause** the legal requirements for data transfers from the EU **to be uncertain.** ~~under other legal mechanisms and has resulted in some~~ EU data protection authorities **have and may again** ~~blocking~~ --- **block** the use of **certain** U. S.- based services that involve the transfer of data to the U. S. **In** ~~The U. S. and~~ the EU **and** ~~in March 2022 agreed in principle on a replacement framework for the~~ **other markets** ~~Privacy Shield~~ , ~~called the Trans- Atlantic Data Privacy Framework. A failure of the U. S. and EU to finalize the Trans- Atlantic Data Privacy Framework could compound that uncertainty and result in additional blockages of data transfers. Potential~~ **potential** new rules and restrictions on the flow of data across borders could increase the cost and complexity of delivering our products and services ~~in some markets~~ . ~~For example~~ **In addition** , the EU General Data Protection Regulation (" GDPR ") **, which** applies to all of our activities conducted from an establishment in the EU or related to products and services offered in the EU, imposes a range of compliance obligations regarding the handling of personal data. More recently, the EU has been developing new requirements related to the use of data, including in the Digital Markets Act, the Digital Services Act, and the Data Act, that ~~will~~ add additional rules and restriction on the use of data in our products and services. Engineering efforts to build and maintain capabilities to facilitate compliance with these laws involve substantial expense and the diversion of engineering resources from other projects. We might experience reduced demand for our offerings if we are unable to engineer products that meet our legal duties or help our customers meet their obligations under ~~the~~ **these** ~~GDPR~~ and other data regulations, or if our implementation to comply ~~with the GDPR~~ makes our offerings less attractive. Compliance with these obligations depends in part on how particular regulators interpret and apply them. If we fail to comply, or if regulators assert we have failed to comply (including in response to complaints made by customers), it may lead to regulatory enforcement actions, which can result in **significant** monetary penalties ~~(of up to 4 % of worldwide revenue in the case of GDPR)~~ , private lawsuits, reputational damage, blockage of international data transfers, and loss of customers. The highest fines assessed under GDPR have recently been increasing, especially against large technology companies. Jurisdictions around the world, such as China, India, and states in the U. S. have adopted, or are considering adopting or expanding, laws and regulations imposing obligations regarding the **collection,** handling ~~or~~ **, and** transfer of personal data. **Our** ~~The Company' s~~ investment in gaining insights from data is becoming central to the value of the services **, including AI services,** we deliver to customers, to ~~our~~ operational efficiency and key opportunities in monetization, **and to** customer perceptions of quality ~~, and operational efficiency~~ . Our ability to use data in this way may be constrained by regulatory developments that impede realizing the expected return from this investment. Ongoing legal analyses, reviews, and inquiries by regulators of Microsoft practices, or relevant practices of other organizations, may result in burdensome or inconsistent requirements, including data sovereignty and localization requirements, affecting the location, movement, collection, and use of our customer and internal employee data as well as the management of that data. Compliance with applicable laws and regulations regarding personal data may require changes in services, business practices, or internal systems that result in increased costs, lower revenue, reduced efficiency, or greater difficulty in competing with foreign- based firms. Compliance with data regulations might limit our ability to innovate or offer certain features and functionality in some jurisdictions where we operate. Failure to comply with existing or new rules may result in significant penalties or orders to stop the alleged noncompliant activity, as well as negative publicity and diversion of management time and effort. **Other regulatory areas that may apply to** our products and online services offerings **include** ~~,and those that impose~~ requirements related to user privacy,telecommunications,data storage and protection,advertising,and online content. **For example,some regulators are taking the position that our offerings such as Microsoft Teams and Skype are covered by existing** ~~Laws~~ **laws** ~~in several jurisdictions~~ **regulating telecommunications services,and some new laws** ,including EU Member State laws under the European Electronic Communications Code, ~~increasingly define certain~~ **are defining more** of our services as regulated telecommunications services.This trend may continue and will result in these offerings being subjected to additional data protection,security, **and** law enforcement surveillance ~~,and other~~ obligations.Regulators ~~and private litigants~~ may assert that our collection,use,and management of customer data and other information is inconsistent with their laws and regulations,including laws that apply to the tracking of users via technology such as cookies. ~~New environmental,social,and governance laws and regulations are expanding mandatory disclosure,reporting,and diligence requirements.~~ Legislative or regulatory action relating to cybersecurity requirements may increase the costs to develop,implement,or secure our products and services ~~.Compliance with evolving digital accessibility laws and standards will require engineering and is important to our efforts to empower all people and organizations to achieve more~~ .Legislative and regulatory action is emerging in the areas of AI and content moderation,which could increase costs or restrict opportunity. **Applying** ~~For example,in the EU,an AI Act is being considered,and may entail increased costs or decreased opportunities for the operation of our AI services in the European market.How~~ these laws and regulations ~~apply~~ to our business is often unclear,subject to change over time,and sometimes may **conflict** ~~be inconsistent~~ from jurisdiction to jurisdiction. **Additionally** ~~In addition~~ , **these laws and** governments' approach to **their** enforcement,and our products and services,are continuing to evolve.Compliance with **these types of** ~~existing,expanding,or new laws and regulations~~ **regulation** may involve significant costs or require changes in products or business practices that ~~could adversely affect our results~~ **result** ~~of operations~~ **in reduced revenue** .Noncompliance could result in the imposition of penalties or orders we ~~cease~~ **stop** the alleged noncompliant activity. ~~In addition~~ **We strive to empower all people and organizations to achieve more** , **and accessibility of our products is an important aspect of this goal.** ~~there~~ **There** is increasing pressure from advocacy **groups,regulators,competitors,customers,and other stakeholders to make technology more accessible.If our products do not meet customer expectations or global accessibility requirements,we could lose sales opportunities or face regulatory or legal actions.** We have claims and lawsuits against us that may result in adverse outcomes. We are subject to a variety of claims and lawsuits. These claims may arise from a wide variety of business practices and initiatives, including major new product releases such as Windows, **AI services,** significant business transactions, warranty or product claims, ~~and~~ employment practices **, and regulation** . Adverse outcomes in some or all of these claims may result in significant monetary damages or injunctive relief that could adversely affect our ability to conduct our business. The litigation and other claims are subject to inherent uncertainties and management' s view of these matters may change in the future. A material adverse impact in our consolidated financial statements could occur for the period in which the effect of an unfavorable outcome becomes probable and reasonably estimable. Our business with government customers may present additional uncertainties. We derive substantial revenue from government contracts. Government contracts generally can present risks and challenges not present in private commercial agreements. For instance, we may be subject to government audits and investigations relating to these contracts, we could be suspended or debarred as a governmental contractor, we could incur civil and criminal fines and penalties, and under certain circumstances contracts may be rescinded. Some agreements may allow a government to terminate without cause and provide for higher liability limits for certain losses. Some contracts may be subject to periodic funding approval, reductions **, cancellations** , or delays which could adversely impact public- sector demand for our products and services. These events could negatively impact our results of operations, financial condition, and reputation. We may have additional tax liabilities. We are subject to income taxes in the U. S. and many foreign jurisdictions. Significant judgment is required in determining our worldwide provision for income taxes. In the course of our business, there are many transactions and calculations where the ultimate tax determination is uncertain. For example, compliance with the 2017 United States Tax Cuts and Jobs Act (" TCJA ") and possible future legislative changes may require the collection of information not regularly produced within the ~~Company~~ **company** , the use of estimates in our consolidated financial statements, and the exercise of significant judgment in accounting for its provisions. As regulations and guidance evolve with respect to the TCJA or possible future legislative changes, and as we gather more information and perform more analysis, our results may differ from previous estimates and may materially affect our consolidated financial statements. We **are** regularly ~~are~~ under audit by tax authorities in different jurisdictions. Although we believe that our provision for income taxes and our tax estimates are reasonable, tax authorities may disagree with certain positions we have taken. In addition, economic and political pressures to increase tax revenue in various jurisdictions may make resolving tax disputes favorably more difficult. We are currently under Internal Revenue Service audit for prior tax years, with the primary unresolved issues relating to transfer pricing. The final resolution of those audits, and other audits or litigation, may differ from the amounts recorded in our consolidated financial statements and may materially affect our consolidated financial statements in the period or periods in which that determination is made. We earn a significant amount of our operating income outside the U. S. A change in the mix of earnings and losses in countries with differing statutory tax rates, changes in our business or structure, or the expiration of or disputes about certain tax agreements in a particular country may result in higher effective tax rates for the ~~Company~~ **company** . In addition, changes in U. S. federal and state or international tax laws applicable to corporate multinationals, other fundamental law changes currently being considered by many countries, including in the U. S., and changes in taxing jurisdictions' administrative interpretations, decisions, policies, and positions may materially adversely impact our consolidated financial statements. INTELLECTUAL PROPERTY RISKS We **face risks related to the protection and utilization of our intellectual property that** may ~~not~~ **result in our business and operating results may** be **harmed. Protecting our intellectual property rights and combating unlicensed copying and use of our software and other intellectual property on a global basis is difficult. Similarly, the absence of harmonized patent laws makes it more difficult to ensure consistent respect for patent rights. Changes in the law may continue to weaken our ability to prevent the use of patented technology or collect revenue for licensing our patents. Additionally, licensees of our patents may fail to satisfy their obligations to pay us royalties or may contest the scope and extent of their obligations. Finally, our increasing engagement with open source software will also cause us to license our intellectual property rights broadly in certain situations. If we are** ~~able~~ **unable** to protect our **intellectual property, our revenue may be adversely affected** ~~source code from copying if there is an unauthorized disclosure~~ . Source code, the detailed program commands for our operating systems and other software programs, is critical to our business ~~. Although we license portions of our application and operating system source code to several licensees, we take significant measures to protect the secrecy of large portions of our source code~~ . If our source code leaks, we might lose future trade secret protection for that code. It may then become easier for third parties to compete with our products by copying functionality, which could adversely affect our revenue and operating ~~margins~~ **results** . Unauthorized disclosure of source code also could increase the security risks described elsewhere in these risk factors. ~~Legal~~

~~changes, our evolving business model, piracy, and other factors may decrease the value of our intellectual property. Protecting our intellectual property rights and combating unlicensed copying and use of our software and other intellectual property on a global basis is difficult. While piracy adversely affects U. S. revenue, the impact on revenue from outside the U. S. is more significant, particularly countries in which the legal system provides less protection for intellectual property rights. Our revenue in these markets may grow more slowly than the underlying device market. Similarly, the absence of harmonized patent laws makes it more difficult to ensure consistent respect for patent rights. Throughout the world, we educate users about the benefits of licensing genuine products and obtaining indemnification benefits for intellectual property risks, and we educate lawmakers about the advantages of a business climate where intellectual property rights are protected. Reductions in the legal protection for software intellectual property rights could adversely affect revenue. We expend significant resources to patent the intellectual property we create with the expectation that we will generate revenues by incorporating that intellectual property in our products or services or, in some instances, by licensing or cross- licensing our patents to others in return for a royalty and / or increased freedom to operate. Changes in the law may continue to weaken our ability to prevent the use of patented technology or collect revenue for licensing our patents. These include legislative changes and regulatory actions that make it more difficult to obtain injunctions, and the increasing use of legal process to challenge issued patents. Similarly, licensees of our patents may fail to satisfy their obligations to pay us royalties or may contest the scope and extent of their obligations. The royalties we can obtain to monetize our intellectual property may decline because of the evolution of technology, price changes in products using licensed patents, greater value from cross- licensing, or the difficulty of discovering infringements. Finally, our increasing engagement with open source software will also cause us to license our intellectual property rights broadly in certain situations and may negatively impact revenue.~~ Third parties may claim **that** we infringe their intellectual property ~~rights~~. From time to time, others claim we infringe their intellectual property rights ~~. The number of these claims may grow because of constant technological change in the markets in which we compete, the extensive patent coverage of existing technologies, the rapid rate of issuance of new patents, and our offering of first- party devices, such as Surface~~. To resolve these claims, we may enter into royalty and licensing agreements on terms that are less favorable than currently available, stop selling or redesign affected products or services, or pay damages to satisfy indemnification commitments with our customers. ~~These~~ **Adverse** outcomes **could also include** ~~may cause operating margins to decline. Besides money~~ **monetary** damages **or** ~~, in some jurisdictions plaintiffs can seek~~ injunctive relief that may limit or prevent importing, marketing, and selling our products or services that have infringing technologies ~~. In some countries, such as Germany, an injunction can be issued before the parties have fully litigated the validity of the underlying patents~~. We have paid significant amounts to settle claims related to the use of technology and intellectual property rights and to procure intellectual property rights as part of our strategy to manage this risk, and may continue to do so. GENERAL RISKS If our reputation or our brands are damaged, our business and operating results may be harmed. Our reputation and brands are globally recognized and are important to our business. Our reputation and brands affect our ability to attract and retain consumer, business, and public- sector customers. There are numerous ways our reputation or brands could be damaged. These include product safety or quality issues, our environmental impact and sustainability, supply chain practices, or human rights record. We may experience backlash from customers, government entities, advocacy groups, employees, and other stakeholders that disagree with our product offering decisions or public policy positions. Damage to our reputation or our brands may occur from, among other things: • The introduction of new features, products, services, or terms of service that customers, users, or partners do not like. • Public scrutiny of our decisions regarding user privacy, data practices, or content. • Data security breaches, compliance failures, or actions of partners or individual employees. The proliferation of social media may increase the likelihood, speed, and magnitude of negative brand events. If our brands or reputation are damaged, it could negatively impact our revenues or margins, or ability to attract the most highly qualified employees. Adverse economic or market conditions may harm our business. Worsening economic conditions, including inflation, recession, pandemic, or other changes in economic conditions, may cause lower IT spending and adversely affect our revenue. If demand for PCs, servers, and other computing devices declines, or consumer or business spending for those products declines, our revenue will be adversely affected. Our product distribution system relies on an extensive partner and retail network. OEMs building devices that run our software have also been a significant means of distribution. The impact of economic conditions on our partners, such as the bankruptcy of a major distributor, OEM, or retailer, could cause sales channel disruption. Challenging economic conditions also may impair the ability of our customers to pay for products and services they have purchased. As a result, allowances for doubtful accounts and write- offs of accounts receivable may increase. We maintain an investment portfolio of various holdings, types, and maturities. These investments are subject to general credit, liquidity, market, and interest rate risks, which may be exacerbated by market downturns or events that affect global financial markets. A significant part of our investment portfolio comprises U. S. government securities. If global financial markets decline for long periods, or if there is a downgrade of the U. S. government credit rating due to an actual or threatened default on government debt, our investment portfolio may be adversely affected and we could determine that more of our investments have experienced a decline in fair value, requiring impairment charges that could adversely affect our consolidated financial statements. Catastrophic events or geopolitical conditions may disrupt our business. A disruption or failure of our systems or operations because of a major earthquake, weather event, cyberattack, terrorist attack, pandemic, or other catastrophic event could cause delays in completing sales, providing services, or performing other critical functions. Our corporate headquarters, a significant portion of our research and development activities, and certain other essential business operations are in the Seattle, Washington area, and we have other business operations in the Silicon Valley area of California, both of which are seismically active regions. A catastrophic event that results in the destruction or disruption of any of our critical business or IT systems, or the infrastructure or systems they rely on, such as power grids, could harm our ability to conduct normal business operations. Providing our customers with more services and solutions in the cloud puts a premium on the resilience of our systems and strength of our business continuity management plans and magnifies the potential impact of prolonged service outages in our consolidated financial statements.

Abrupt political change, terrorist activity, and armed conflict, such as the ongoing conflict in Ukraine, pose a risk of general economic disruption in affected countries, which may increase our operating costs and negatively impact our ability to sell to and collect from customers in affected markets. These conditions also may add uncertainty to the timing and budget for technology investment decisions by our customers and may cause supply chain disruptions for hardware manufacturers. Geopolitical change may result in changing regulatory systems and requirements and market interventions that could impact our operating strategies, access to national, regional, and global markets, hiring, and profitability. Geopolitical instability may lead to sanctions and impact our ability to do business in some markets or with some public- sector customers. Any of these changes may negatively impact our revenues. The occurrence of regional epidemics or a global pandemic **,** such as COVID- 19 **,** may adversely affect our operations, financial condition, and results of operations ~~. The COVID- 19 pandemic has had widespread, rapidly evolving, and unpredictable impacts on global society, economies, financial markets, and business practices~~ . The extent to which global pandemics impact our business going forward will depend on factors such as the duration and scope of the pandemic; governmental, business, and individuals' actions in response to the pandemic; and the impact on economic activity **,** including the possibility of recession or financial market instability. Measures to contain a global pandemic may intensify other risks described in these Risk Factors. ~~Any of these measures may adversely impact our ability to: • Maintain our operations infrastructure, including the reliability and adequate capacity of cloud services. • Satisfy our contractual and regulatory compliance obligations as we adapt to changing usage patterns, such as through datacenter load balancing. • Ensure a high-quality and consistent supply chain and manufacturing operations for our hardware devices and datacenter operations. • Effectively manage our international operations through changes in trade practices and policies. • Hire and deploy people where we most need them. • Sustain the effectiveness and productivity of our operations including our sales, marketing, engineering, and distribution functions.~~ We may incur increased costs to effectively manage these aspects of our business. If we are unsuccessful **,** it may adversely impact our revenues, cash flows, market share growth, and reputation. The long- term effects of climate change on the global economy and the IT industry in particular are unclear. Environmental regulations or changes in the supply, demand **,** or available sources of energy or other resources may affect the availability or cost of goods and services, including natural resources, necessary to run our business. Changes in climate where we operate may increase the costs of powering and cooling computer hardware we use to develop software and provide cloud- based services. Our global business exposes us to operational and economic risks. Our customers are located throughout the world and a significant part of our revenue comes from international sales. The global nature of our business creates operational, economic, and geopolitical risks. Our results of operations may be affected by global, regional, and local economic developments, monetary policy, inflation, and recession, as well as political and military disputes. In addition, our international growth strategy includes certain markets, the developing nature of which presents several risks, including deterioration of social, political, labor, or economic conditions in a country or region, and difficulties in staffing and managing foreign operations. Emerging nationalist and protectionist trends and concerns about human rights **, the environment,** and political expression in specific countries may significantly alter the trade and commercial environments. Changes to trade policy or agreements as a result of populism, protectionism, or economic nationalism may result in higher tariffs, local sourcing initiatives, and non- local sourcing restrictions, export controls, investment restrictions, or other developments that make it more difficult to sell our products in foreign countries. Disruptions of these kinds in developed or emerging markets could negatively impact demand for our products and services **, impair our ability to operate in certain regions,** or increase operating costs. Although we hedge a portion of our international currency exposure, significant fluctuations in foreign exchange rates between the U. S. dollar and foreign currencies may adversely affect our results of operations. Our business depends on our ability to attract and retain talented employees. Our business is based on successfully attracting and retaining talented employees representing diverse backgrounds, experiences, and skill sets. The market for highly skilled workers and leaders in our industry is extremely competitive. Maintaining our brand and reputation, as well as a diverse and inclusive work environment that enables all our employees to thrive, are important to our ability to recruit and retain employees. We are also limited in our ability to recruit internationally by restrictive domestic immigration laws. Changes to U. S. immigration policies that restrain the flow of technical and professional talent may inhibit our ability to adequately staff our research and development efforts. If we are less successful in our recruiting efforts, or if we cannot retain highly skilled workers and key leaders, our ability to develop and deliver successful products and services may be adversely affected. Effective succession planning is also important to our long- term success. Failure to ensure effective transfer of knowledge and smooth transitions involving key employees could hinder our strategic planning and execution. How employment- related laws are interpreted and applied to our workforce practices may result in increased operating costs and less flexibility in how we meet our workforce needs. Our global workforce is ~~primarily~~ **predominantly** non- unionized, ~~but~~ **although** we **do** have ~~several~~ **some employees in the U. S. and internationally who are represented by** unions ~~and~~ **or** works councils ~~outside of the United States~~ . In the U. S., there has been a general increase in workers exercising their right to form or join a union. **The** ~~While Microsoft has not received such petitions in the U. S., the~~ unionization of significant employee populations could result in higher costs and other operational changes necessary to respond to changing conditions and to establish new relationships with worker representatives.