Software Quality Issues in the U.S. Cost an Estimated $2.41 Trillion in 2022

Synopsys-sponsored CISQ report finds existing vulnerabilities, software supply chain complexities and growing impact of technical debt as key drivers of increased cyberattacks, cost

MOUNTAIN VIEW, Calif., Dec. 6, 2022 /PRNewswire/ -- Synopsys, Inc. (Nasdaq: SNPS) today revealed that software quality issues may have held the U.S. economy back to the tune of $2.41 trillion in 2022. This statistic is unearthed in "The Cost of Poor Software Quality in the US: A 2022 Report." The report's findings reflect that as of 2022, the cost of poor software quality in the U.S.—which includes cyber-attacks due to existing vulnerabilities, complex issues involving the software supply chain, and the growing impact of rapidly accumulating technical debt—have led to a build-up of historic software deficiencies.

Co-sponsored by Synopsys, the report was produced by the Consortium for Information & Software Quality (CISQ), an organization developing international standards to automate software quality measurement and promoting the development and maintenance of secure, reliable, and trustworthy software.

"Cybercrime is predicted to cost the world $7 trillion in 2022," said report author, Herb Krasner, retired Professor of Software Engineering, University of Texas at Austin. "With that top of mind, 'The Cost of Poor Software Quality in the US: A 2022 Report' offers practical advice and specific guidance for software engineers, project teams, and organizational leaders to proactively improve the quality of the software they use and build. Now is the time to turn our attention to recent developments and emerging solutions to help improve the poor software quality situation as it now exists and stabilize and reduce the growth rate of CPSQ in the near future."

The report highlights several key areas of CPSQ growth, including:

- **Cybercrime losses due to a rising number of software vulnerabilities** Losses rose 64% from 2020 to 2021, and are on track for a further 42% increase from 2021 to 2022. The quantity and cost of cybercrime incidents have been on the rise for over a decade, and now account for a sum equivalent to the world's third largest economy after the U.S. and China.
- **Software supply chain problems with underlying third-party components are up significantly**. This year's report shows that the number of failures due to weaknesses in open source software components accelerated by an alarming 650% from 2020 to 2021.
- **Technical debt has become the largest obstacle to making changes in existing code bases** Technical debt refers to software development rework costs from the accumulation of deficiencies leaving data and systems potentially vulnerable. This year's report illustrates that deficiencies aren't being resolved, leading technical debt to increase to approximately $1.52 trillion.

"In today's complex software supply chain, just because a newly-added open source component is secure today, does not mean that it will be secure tomorrow," said Dr. Anita D'Amico, Synopsys Software Integrity Group VP of Cross-Portfolio Solutions and Strategy and CISQ Board Member. "Creating a software Bill of Materials (SBOM) allows organizations to proactively gather a comprehensive inventory of the components used to make up a piece of software. That means when a new vulnerability is identified in an existing component, organizations can quickly identify where it is in their software and take action to remedy it."

The report also found that operational failures, primarily due to cyber-attacks and open source deficiencies, have risen alongside technical debt as deficiencies aren't being resolved at a comparable rate. With these rises, developments in technologies and practices to remediate issues have also matured considerably in recent years. Using software quality standards in association with related tooling solutions, assessing and monitoring third party and open source components, and applying patches in a timely manner are all key strategies in reducing CPSQ.

To learn more, download a copy of The Cost of Poor Software Quality in the US: A 2022 Report or read our blog post highlighting the report's key takeaways.

About the Synopsys Software Integrity Group

Synopsys Software Integrity Group provides integrated solutions that transform the way development teams build and deliver software, accelerating innovation while addressing business risk. Our industry-leading portfolio of software security products and services is the most comprehensive in the world and interoperates with third-party and open source tools, allowing organizations to leverage existing investments to build the security program that's best for them. Only Synopsys offers everything you need to build trust in your software. Learn more at www.synopsys.com/software.

About Synopsys

Synopsys, Inc. (Nasdaq: SNPS) is the Silicon to Software™ partner for innovative companies developing the electronic products and software applications we rely on every day. As an S&P 500 company, Synopsys has a long history of being a global leader in electronic design automation (EDA) and semiconductor IP and offers the industry's broadest portfolio of application security testing tools and services. Whether you're a system-on-chip (SoC) designer creating advanced semiconductors, or a software developer writing more secure, high-quality code, Synopsys has the solutions needed to deliver innovative products. Learn more at www.synopsys.com.

Editorial Contact:
Liz Samet
Synopsys, Inc.
336-414-6753
esamet@synopsys.com

SOURCE Synopsys, Inc.