Synopsys-Sponsored CISQ Research Estimates Cost of Poor Software Quality in the US $2.08 Trillion in 2020

Many digital transformation efforts fail due to poor software engineering practices around insufficient computing performance, poor cybersecurity and unscalable architectures.

MOUNTAIN VIEW, Calif., Jan. 6, 2021 /PRNewswire/ -- Synopsys, Inc. (Nasdaq: SNPS) today announced the publication of The Cost of Poor Software Quality In the US: A 2020 Report. Co-sponsored by Synopsys, the report was produced by the Consortium for Information & Software Quality (CISQ), an organization which develops international standards to automate software quality measurement and promotes the development and sustainment of secure, reliable, and trustworthy software. The report's findings reflect that the cost of poor software quality (CPSQ) in the US in 2020 was approximately $2.08 trillion. This includes poor software quality resulting from software failures, unsuccessful development projects, legacy system problems, technical debt and cybercrime enabled by exploitable weaknesses and vulnerabilities in software.

"As organizations undertake major digital transformations, software-based innovation and development rapidly expands," said report author, Herb Krasner. "The result is a balancing act, trying to deliver value at high speed without sacrificing quality. However, software quality typically lags behind other objectives in most organizations. That lack of primary attention to quality comes at a steep cost. For this reason, this report offers specific recommendations to software engineers, project teams and organizational leaders to improve the quality of the software they use and build."

Key findings from the report include:

- **Operational software failure is the leading driver of the total cost of poor software quality (CPSQ), estimated at $1.56 trillion**. This figure represents a 22% increase since 2018. That number could be low given the meteoric rise in cybersecurity failures, and also with the understanding that many failures go unreported. Cybercrimes enabled by exploitable weaknesses and vulnerabilities in software are the largest growth area by far in the last 2 years. The underlying cause is primarily unmitigated software flaws.
- **Unsuccessful development projects, the next largest growth area of the CPSQ, is estimated at $260 billion.** This figure has risen by 46% since 2018. There has been a steady project failure rate of ~19% for over a decade. The underlying causes are varied, but one consistent theme has been the lack of attention to quality. Research suggests that success rates go up dramatically when using Agile and DevOps methodologies, leading to decision latency being minimized.
- **The operation and maintenance of legacy software contributed $520 billion to the CPSQ.** While this is down from $635 billion in 2018, it still represents nearly a third of the US's total IT expenditure in 2020.

"As poor software quality persists on an upward trajectory, the solution remains the same: prevention is still the best medicine. It's important to build secure, high-quality software that addresses weaknesses and vulnerabilities as close to the source as possible," said Joe Jarzombek, Director for Government and Critical Infrastructure Programs at Synopsys. "This limits the potential damage and cost to resolve issues. It reduces the cost of ownership and makes software-controlled capabilities more resilient to attempts of cyber exploitation."

Methodologies such as Agile and DevOps have supported the evolution of software development whereby software developers apply enhancements as small, incremental changes that are tested and committed daily, hourly, or even moment by moment into production. This results in higher velocity and more responsive development cycles, but not necessarily better quality. As DevSecOps aims to improve the security mechanisms around high-velocity software development, the emergence of DevQualOps encompasses activities that assure an appropriate level of quality across the Agile, DevOps, and DevSecOps lifecycle.

To learn more, download a copy of the The Cost of Poor Software Quality In the US: A 2020 Report, read our new blog post highlighting the report's key takeaways, or register for the January 27 webinar.

About the Synopsys Software Integrity Group

Synopsys Software Integrity Group helps development teams build secure, high-quality software, minimizing risks while maximizing speed and productivity. Synopsys, a recognized leader in application security, provides static analysis, software composition analysis, and dynamic analysis solutions that enable teams to quickly find and fix vulnerabilities and defects in proprietary code, open source components, and application behavior. With a combination of industry-leading tools, services, and expertise, only Synopsys helps organizations optimize security and quality in DevSecOps and throughout the software development life cycle. 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 the world's 15th largest software company, Synopsys has a long history of being a global leader in electronic design automation (EDA) and semiconductor IP and is also growing its leadership in software security and quality solutions. Whether you're a system-on-chip (SoC) designer creating advanced semiconductors, or a software developer writing applications that require the highest security and quality, Synopsys has the solutions needed to deliver innovative, high-quality, secure products. Learn more at www.synopsys.com.

Editorial Contact:
Mark Van Elderen
Synopsys, Inc.
650-793-7450
mark.vanelderen@synopsys.com

SOURCE Synopsys, Inc.