SECUREKLOUD
SecureKloud Technologies Limited
(Formerly 8K Miles Software Services Limited)

Ref: SK/CHN/2023-24/E15

July 12, 2023

National Stock Exchange of India Limited Capital Market – Listing, Exchange Plaza, 5th Floor, Plot No. C/1 G Block, Bandra – Kurla Complex, Bandra (E), Mumbai 400 051	BSE Limited 25th Floor, Phiroze Jeejeebhoy Towers Dalal Street, Fort Mumbai 400001
EQ-SECURKLOUD – ISIN – INE650K01021	Scrip code: 512161 – ISIN – INE650K01021

Dear Sir/ Madam,

Subject: Press Release – Healthcare Triangle Inc launches ransomware initiative aimed at protection and prevention for healthcare providers

Healthcare Triangle Inc, step-down subsidiary of SecureKloud Technologies Limited, has announced its launch of a new initiative aimed at preparing healthcare organisations with critical tools and guidance for preventing and responding to ransomware incidents.

This is for your information and records.

Thanking you,

Yours Truly
For SecureKloud Technologies Limited

ROSHINI SELVAKUMAR
Digitally signed by ROSHINI SELVAKUMAR
Date: 2023.07.12 18:29:15 +05'30'

SECUREKLOUD TECHNOLOGIES LIMITED ★ CHENNAI

Roshini Selvakumar
Company Secretary and Compliance Officer

Healthcare Triangle Launches Ransomware Initiative Aimed at Protection and Prevention for Healthcare Providers

Company to educate and guide best practices for maintaining resiliency in the face of increasing ransomware attacks in healthcare

PLEASANTON, Calif., July 12, 2023 (GLOBENEWSWIRE) -- Healthcare Triangle, Inc (Nasdaq: HCTI) ("HCTI" or the "Company"), a leader in digital transformation solutions including managed services, cloud enablement, and data analytics for the healthcare and life sciences industries, today announced its launch of a new initiative aimed at preparing healthcare organizations with critical tools and guidance for preventing and responding to ransomware incidents.

Ransomware attacks on the U.S. healthcare sector have more than doubled from 2016 to 2021 and have exposed confidential and protected medical information of nearly 42 million patients.[1] Most recently, CalPERS and CalSTRS, the nation's two largest public pension funds, were attacked with a data breach that exposed personal information on 1.2 million government retirees and beneficiaries. In May, Johns Hopkins University and Johns Hopkins Health experienced a similar cyberattack and data breach. Both incidents have been attributed to a Russian hacker group known as the Cl0p ransomware syndicate. Meanwhile, while large institutions and healthcare systems address major attacks, rural hospitals particularly vulnerable to risk are facing significant budget constraints for ransomware protection and need assistance from the federal government. In response, U.S. Senator Josh Hawley's "Rural Hospital Cybersecurity Enhancement Act" passed through committee on June 14, 2023, and now heads to the Senate floor. Healthcare Triangle applauds this and other actions by the U.S. Congress to address the growing threat of ransomware attacks, including the work of the Joint Ransomware Task Force (JRTF), an interagency effort to reduce ransomware.

Lena Kannappan, head of business, strategy and partnerships for Healthcare Triangle, stated, "Generative AI and data modernization technologies can play a key role in improving patient outcomes and streamlining healthcare operations. However, looming ransomware threats can severely impact patient care, disrupt operations, cause financial losses, put community lives at risk, and force hospitals to shutter operations. With our new ransomware initiative, our Company's goal is to take a proactive leadership role in educating and equipping rural hospitals, community hospitals, and large health systems in need with critical resources for improving their preparedness, prevention, detection, response, and recovery from ransomware incidents. We are engaged in discussions with several healthcare systems about this initiative and look forward to raising awareness and delivering robust, best-in-class solutions throughout the healthcare and life sciences industries."

Participants in Healthcare Triangle's ransomware initiative will benefit from three key learning topics about artificial intelligence, machine learning, and ransomware challenges.

1. Key Learning #1 – The crucial role of incident response planning, testing, and the role each person plays in minimizing the impact of ransomware attacks to improve basic cybersecurity hygiene in healthcare.
2. Key Learning #2 – Effective strategies for preparing for and preventing ransomware.

[1] Journal of the American Medical Association (JAMA). Trends in Ransomware Attacks on U.S. Hospitals, Clinics and Other Health Care Delivery Organizations, 2016-2021. December 2022.

3. Key Learning #3 – The criticality of early detection and rapid response phase of ransomware attacks.

Healthcare Triangle's ransomware prevention practices and training services include:

- Education workshops
- Risk assessment
- Recommendations for most effective tools and processes
- Backup and recovery plans
- Multi-factor authentication (MFA)
- Identity management
- Simulated phishing exercises
- Software updates
- Routine risk assessments
- Continuous monitoring
- External partnering
- Measures of effectiveness

Contact the Company for more information: info@healthcaretriangle.com

About Healthcare Triangle

Healthcare Triangle, Inc. based in Pleasanton, California, reinforces healthcare progress through breakthrough technology and extensive industry knowledge and expertise. We support healthcare including hospitals and health systems, payers, and pharma/life sciences organizations in their effort to improve health outcomes through better utilization of the data and information technologies that they rely on. Healthcare Triangle achieves HITRUST Certification for Cloud and Data Platform (CaDP), marketed as CloudEz™ and DataEz™. HITRUST Risk-based, 2-year (r2) Certified status demonstrates to our clients the highest standards for data protection and information security. Healthcare Triangle enables the adoption of new technologies, data enlightenment, business agility, and response to immediate business needs and competitive threats. The highly regulated healthcare and life sciences industries rely on Healthcare Triangle for expertise in digital transformation encompassing the cloud, security and compliance, data lifecycle management, healthcare interoperability, and clinical and business performance optimization. For more information, visit www.healthcaretriangle.com.

Forward-Looking Statements and Safe Harbor Notice

All statements other than statements of historical facts included in this press release are "forward-looking statements" (as defined in the Private Securities Litigation Reform Act of 1995). Such forward-looking statements include our expectations and those statements that use forward-looking words such as "projected," "expect," "possibility" and "anticipate." The achievement or success of the matters covered by such forward-looking statements involve significant risks, uncertainties and assumptions. Actual results could differ materially from current projections or implied results. Investors should read the risk factors set forth in the Company's Prospectus filed with the SEC on October 7, 2021, previous filings, subsequent filings and future periodic reports filed with the SEC. All the Company's forward-looking statements are expressly qualified by all such risk factors and other cautionary statements.

The Company cautions that statements and assumptions made in this news release constitute forward-looking statements and make no guarantee of future performance. Forward-looking statements are based on estimates and opinions of management at the time statements are made.

The information set forth herein speaks only as of the date hereof. The Company and its management undertake no obligation to revise these statements following the date of this news release.

Contacts

Media:
Michael Campana
michael.c@healthcaretriangle.com

Investors:
1-800-617-9550
ir@healthcaretriangle.com