CYBEATS

Cybeats Addresses Recent '3CX' Cyberattack and Highlights Government Agencies' Support for SBOMs

TORONTO, April 13, 2023 /CNW/ - **Cybeats Technologies Corp. ("Cybeats" or the "Company")** (CSE: CYBT) (OTCQB: CYBCF) highlights the challenges faced by nations in securing their infrastructure, particularly in the context of increasing software supply chain threats. The recent 3CX cyberattack carried out by North Korea nation state-backed hackers has public and private stakeholders calling for increased supply chain transparency.

In line with the tone set by the Cyber Executive Order (EO) 14028 from 2021[1], government agencies around the world are recognizing Software Bills of Materials (SBOM) as a required baseline to ensure security in software acquisition, market access and risk management processes. The recently released U.S. National Cyber Strategy (NCS) builds on SBOM efforts in the Cyber EO calling on U.S. Congress to change market incentives and establish liability for software products and services, and expand SBOM requirements. Cybeats is currently engaged with multiple government agencies responsible for safeguarding national security.

"Government agencies play an important role in ensuring that industry adopts standards of care for secure software development and maintenance of products and services, or face liability risks. As SBOM requirements become increasingly relevant to the government software procurement process, the private sector is rapidly embracing them as well. With the growing significance of SBOMs, organizations spanning diverse industries, such as finance, technology, industrial, medical, and automotive, are actively evaluating their Software Development Life Cycle and SBOM practices to meet the rising demand for SBOMs," said **Yoav Raiter, CEO of Cybeats.**

3CX Software Supply Chain Attack

3CX has over 600,000 customers in 190 countries, representing over 12M users. Security firms have indicated that the 3CX hackers targeted both Windows and macOS users of the compromised 3CX softphone app. The malicious activity includes beaconing to actor-controlled infrastructure, deployment of second-stage payloads, and, in a small number of cases, hands-on-keyboard activity. Initial research indicates the number of potential victims is in the hundreds of thousands.

Cyberattacks like 3CX and SolarWinds have prompted governments globally to collaborate closely with public and private sector security experts and provide additional resources like guidance by the Cybersecurity and Infrastructure Security Agency (CISA) and other U.S. government agencies titled "Securing the Software Supply Chain"[2] for software developers, suppliers and customers, to help ensure a more secure software supply chain. It is becoming imperative for organizations to consistently update their Software Development Life Cycle (SDLC), software and supply chain vulnerability, and risk management resources and practices. SBOM management aims to help mitigate potential vulnerabilities, maintain security and meet compliance requirements.

[1] https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

[2] https://www.cisa.gov/sites/default/files/publications/ESF_SECURING_THE_SOFTWARE_SUPPLY_CHAIN_DEVELOPERS.PDF, 2022 report by the Enduring Security Framework (ESF) Software Supply Chain Working Panel referencing NIST SP 800-218 and other secure software development and supply chain risk management guidance.

SBOM in Canadian Regulations - Bill C-26

Canada's recent introduction of the C-26 legislation outlines the protection of critical cyber systems, laying the groundwork for improved software supply chain security, SBOM, and fostering a safer digital landscape. The Critical Cyber Systems Protection Act (CCSPA) aims to create a framework to protect critical cyber systems that support services vital to national security or public safety. The CCSPA seeks to ensure that risks to critical cyber systems are identified and managed, including risks associated with supply chains and the use of third-party products and services.[3]

This new Canadian legislation follows global trends, focusing on managing risks associated with supply chains and third-party products and services, ensuring that critical cyber systems remain protected from compromise and minimizing the impacts of cybersecurity incidents. Designated operators of these critical cyber systems will be required to establish and implement a cybersecurity program, mitigate supply-chain and third-party risks, and adhere to reporting and notification obligations in the event of a cybersecurity incident.

EU Cyber Resilience Act

Cybercrime costs reached $6 trillion in 2021, prompting the European Commission to propose the Cyber Resilience Act (CRA) to enhance software security. The CRA aims to hold manufacturers accountable for improving software security throughout the entire product life cycle and increase transparency into software vulnerabilities. A key strategy in the CRA is the implementation of Software Bill of Materials (SBOM) management, which tracks and shares metadata details of software components and supply chain relationships. Non-compliance with the CRA may lead to significant fines and reputational damage. As the CRA impacts software sold or used in Europe, adopting SBOM management now is crucial for future compliance and security.[4]

[3] https://www.justice.gc.ca/eng/csj-sjc/pl/charter-charte/c26_1.html

[4] https://www.cybeats.com/blog/why-sboms-are-critical-to-complying-with-the-eu-cyber-resilience-act

About Cybeats

Cybeats is a cybersecurity company providing SBOM management and software supply chain intelligence technology, helping organizations to manage risk, meet compliance requirements, and secure their software from procurement to development and operation. Our platform gives customers comprehensive visibility and transparency into their software supply chain, enabling them to improve operational efficiency and increase revenue. Cybeats. Software Made Certain. Website: https://cybeats.com

SUBSCRIBE: For more information, or to subscribe to the Company's mail list, visit: https://www.cybeats.com/investors

Forward-looking Information Cautionary Statement

Except for statements of historic fact, this news release contains certain "forward-looking information" within the meaning of applicable securities law. Forward-looking information is frequently characterized by words such as "plan", "expect", "project", "intend", "believe", "anticipate", "estimate" and other similar words, or statements that certain events or conditions "may" or "will" occur. Forward-looking statements are based on the opinions and estimates at the date the statements are made, and are subject to a variety of risks and uncertainties and other factors that could cause actual events or results to differ materially from those anticipated in the forward-looking statements including, but not limited to delays or uncertainties with regulatory approvals, including that of the CSE. There are uncertainties inherent in forward-looking information, including factors beyond the Company's control. There are no assurances that the commercialization plans for the products described in this news release will come into effect on the terms or time frame described herein. The Company undertakes no obligation to update forward-looking information if circumstances or management's estimates or opinions should change except as required by law. The reader is cautioned not to place undue reliance on forward-looking statements. Company filings are available at sedar.com.

View original content to download multimedia:
https://www.prnewswire.com/news-releases/cybeats-addresses-recent-3cx-cyberattack-and-highlights-government-agencies-support-for-sboms-301796416.html

SOURCE Cybeats Technologies Corp.

View original content to download multimedia: http://www.newswire.ca/en/releases/archive/April2023/13/c6796.html

%SEDAR: 00031378E

For further information: James Van Staveren, Corporate Development, Phone: 1-888-713-SBOM (7266), Email: ir@cybeats.com

CO: Cybeats Technologies Corp.

CNW 03:00e 13-APR-23