Relay to Host the 'Roots of SBOM' for Their Second Live Webinar on the State of Cybersecurity Industry

Toronto, Ontario--(Newsfile Corp. - August 26, 2021) - Relay Medical Corp. (CSE: **RELA)** **(**OTCQB: **RYMDF) (**FSE: **EIY2**) ("**Relay**" or the "**Company**") is pleased to host the second episode about the "State of Cybersecurity Industry: Roots of SBOM"[1] featuring key panelists Kate Stewart, Steve Springett, Chris Blask and moderated by Evgeniy Kharam. As leaders in SBOMs, these panelists will discuss how crucial they are for protecting technology globally. The event will be hosted live on the Cybeats YouTube[2] channel on September 9th at 1pm EDT.

Relay's Cybeats will host the panel which will feature many industry leaders including **Kate Stewart,** Vice President of Dependable Embedded Systems at The Linux Foundation; she is a world-class innovator and leader in system software and application tools as well as one of the original founders of SPDX. **Steve Springett** is the Chair of CycloneDX SBOM Standard, Core Working Group and World class leader in Defensive Design, Programming and Automation. **Chris Blask,** vice president strategy at Relay, **is a respected** thought leader in SBOMs and is known for creating the Digital Bill of Materials (DBOM) and one of the first commercial firewall products. The panel will be moderated by co-host of the Security Architecture Podcaster, **Evgeniy Kharam.**

Live Webinar Attendees and Date

To view an enhanced version of this graphic, please visit:
https://orders.newsfilecorp.com/files/952/94534_fd5482d9c4c01aed_001full.jpg

Register for the *'Root of SBOM' Free* Webinar using the link below:

https://stateofcybersecurityindustryep.splashthat.com/

As the open-source world continues to grow, panelists will discuss the increasing demand for SBOMs and the greater importance of the longevity and credibility of software ultimately showcasing how it offers a vital solution.

'Economic of Security Adoption' by **Chris Blask**, recently appointed VP of Strategy at Relay:

"At the moment there is a great deal of focus on supply chain security. The mandate to produce or consume Software Bill of Materials (SBOM)[3] *in the U.S. for critical infrastructure is providing fuel to cybersecurity efforts. Transparency is being built into the supply chain to allowthose security needs to be addressed. What many in the security community will miss during this period is that the underlying driver for all these changes is not security, it is* ***economics****. Organizations that adopt these structures before their competitors will find more than improved security. They will find that they have improved logistics, more effective customer relationships, lower costs, and greater profitability. Those who move first in this area will end up out-competing their peers, and that's what history will take note of."*

Transparency and licensing have become increasingly important in the expansion of open source software, thus the need for SBOMs. Now more than ever, it is imperative to think about the sustainability and durability of software. Join us, as we discuss how SBOMs are essential to maintaining the global security of our technology in episode two of the *State of Cybersecurity: The Roots of SBOM* webinar with these leaders in the industry.

"Due to the overwhelmingly positive response for the first Cybeats seminar 'The State of Cybersecurity,' we felt the need to continue the discussion regarding cybersecurity to highlight the importance of SBOMs for global cybersecurity," said Yoav Raiter, CEO of Relay Medical. "SBOMs are the basis of cybersecurity and are of critical importance as the number of connected devices continues to exponentially grow. With cyber-attacks becoming more prevalent, protecting the ever-increasing number of high-value connected devices is now a priority for government regulators, and both large and small organizations which rely on connected technology. We have brought in another leading panel of SBOM experts, and I look forward to a lively discussion with Kate, Steve, and Chris. Please join us for this riveting webinar on September 9 at 1pm ET."

A recent report from Gartner[4] noted that due to the recent increase in cybercrime attacks on information and communication technology (ITC), there must be significant importance placed on operational technology of connected devices. Furthermore, the report indicates that the management of these new cyber risks are either absent or fragmented within most organizations, leaving them exposed.

Examples of recent cybercrimes include the Iowa-based Peoples Community Health Clinic (PCHC), who notified patients about a recent cyberattack which may have impacted patients' private information,[5] and New Jersey-based Bridgeway Senior Healthcare faced a ransomware cybersecurity attack that affected large amounts of patient data.[6]

U.S. Regulators have also taken notice. In May 2021, the U.S. Food & Drug Administration outlined recommendations for cybersecurity standards and guidelines to enhance software supply chain security. The FDA states that increasingly common ransomware attacks on healthcare "highlight the ungraceful failure of perimeter-based firewalls and the safety consequences of not separating operational technology from information technology by design."[7]

On July 12, 2021, U.S Regulators stated new software minimum requirements that apply to software on IoT devices.[8] This news follows the Executive Order (EO) on Improving the Nation's Cybersecurity,[9] as President Biden identified the prevention, detection, assessment and remediation of cyber incidents as a top priority of his Administration. The Commerce Department and National Telecommunications and Information Administration (NTIA) were directed by the EO to publish the minimum elements for a Software Bill of Materials (SBOM), a key tool to help create a transparent and secure software supply chain.[10]

RECENT NEWS: Relay recently announced an engagement with Canada's largest medical technology developer, **StarFish Medical** to provide the Cybeats platform for high-valued connected medical devices. The engagement includes the SBOM software to monitor security of the products being developed and can be licensed by StarFish clients for continued protection. The complete release can be found here: https://bit.ly/2Wn2bV3

SUBSCRIBE: For more information on Relay or to subscribe to the Company's mailing list visit: https://www.relaymedical.com/news

About Cybeats

Cybeats is an integrated security platform designed to secure and protect high-valued connected devices. Cybeats' unique approach eliminates device downtime due to cyber-attacks and allows device manufacturers to develop and maintain secure and protected devices in a timely and cost-efficient manner.

Cybeats' SBOM Studio product allows for the monitoring and analysis of cybersecurity on all components during the design and manufacturing stage, ensuring connected devices have been developed with secure software components.

Cybeats' capabilities span across detecting and mitigating attacks on devices while they are operational, enabling device makers to identify and fix security flaws during the product's design phase and empowering end users with fleet management tools such as secure firmware updates.

Website: www.cybeats.com

About Relay Medical Corp.

Relay Medical is a technology innovator headquartered in Toronto, Canada focused on the development of novel solutions in the diagnostics, AI data science and IoT security sectors.

Website: www.relaymedical.com

Contact:
Destine Lee
Media & Communications
Relay Medical Corp.
Office. 647-872-9982
TF. 1-844-247-6633
Media Inquiries: media@relaymedical.com
Investor Relations: investor.relations@relaymedical.com

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 technology 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. Additional information identifying risks and uncertainties that could affect financial results is contained in the Company's filings with Canadian securities regulators, which filings are available at www.sedar.com.

[1] https://www.linkedin.com/events/6834623376489779200/

[2] https://www.youtube.com/watch?v=jlWPPNuCZTQ

[3] https://en.wikipedia.org/wiki/Software_bill_of_materials

[4] Gartner, "ICT Supply Chain Risk Management Is Mission Critical, but Best Practices Are Just Emerging," Katell Thielemann, 7 July 2021

[5] https://healthitsecurity.com/news/patient-info-exposed-in-health-clinic-cyberattackdata-breach

[6] https://healthitsecurity.com/news/ransomware-extortion-threat-actors-post-data-from-4-healthcare-entities

[7] https://www.fda.gov/media/149954/download

[8] https://www.ntia.gov/blog/2021/ntia-releases-minimum-elements-software-bill-materials

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

[10] https://www.ntia.gov/blog/2021/ntia-releases-minimum-elements-software-bill-materials

To view the source version of this press release, please visit https://www.newsfilecorp.com/release/94534