Cybeats Products Service Security Needs of Large Utility Corporations; Relay Comments on the Economic and National Security Concerns for Utilities Infrastructure

Toronto, Ontario--(Newsfile Corp. - October 8, 2021) - Relay Medical Corp. (**CSE: RELA) (OTCQB: RYMDF) (FSE: EIY2**) ("**Relay**" or the "**Company**") addresses the critical infrastructure sectors of electricity, natural gas, and water, whereby the mitigation of cyber vulnerabilities is of growing national security concern, as well as a cost, IP and compliance issue. Cybeats solutions address the needs of North American utility companies and satisfies new mandated software requirements centered around Software Bill of Materials ("**SBOM**").

In critical utility sectors, software can cost roughly $10,000 USD per line of code and have upwards of 200,000 lines of verification code. This means some organizations have invested billions into their unique software assets, and will need to secure them at all cost. Additionally, governments need to secure utility infrastructure and reduce cyber attack risk for national security and defense. Cybeats helps large utility service providers satisfy regulatory requirements and leverages its technology to detect and eliminate cyber threats in real-time.

"Utility companies face immense cyber risks in the coming years. From national security concerns to increasing costs, North American Utility companies especially will need to implement supply chain security and other cyber defense solutions as soon as possible. Cybeats is actively pursuing commercial partnerships to secure utility infrastructure and software supply chains in the sector. Cybeats is poised to service and secure software supply chains for the various utilities infrastructure sectors," said Dmitry Raidman, co-founder & CTO, Cybeats.

SBOM Importance, National Security

The SBOM inclusion in the executive order was intentionally mandated for the government and private industry, though the two sectors see SBOMs in different ways. Government agencies see SBOMs as a means to reduce national security risks, whereas the private industry might see SBOMs as a cost or economic issue. Private companies will start experiencing pressures to reduce brand reputation risks and protecting IP and trade secrets via SBOM[1] Software vendors can expect to see customers start demanding SBOMs in their contracts.

The U.S. Department of Commerce's National Technology and Information Administration (NTIA) is in the process of launching a pilot program for the energy sector to develop and bring into use a SBOM that could help utilities secure equipment and software, track vulnerabilities and ensure they are patched. Project officials say the effort will build an international, cross-sector effort to establish consensus for the software supply chain technical and operational considerations. Software supply chain attacks are continually becoming more sophisticated as cyber terrorists exploit weaknesses at every step of the software development process.

"SBOM will be an invaluable tool for managing cybersecurity and software supply chain risks," said Allan Friedman, former Director of Cybersecurity Initiatives at NTIA. "We find new vulnerabilities every few months that widely affect a lot of software and embedded components that are really deployed everywhere in our ecosystem- especially in the energy world."

Software supply chain issues are the subject of a new collaboration between the electric power sector and federal government, as past initiatives frequently overlooked electric utility vulnerabilities.[2] The Edison Electric Institute and the North American Transmission Forum have been working with the federal government to pilot the use of SBOMs in the energy sector.[3] If SBOM principles extend to all software, beyond what NIST says is critical, companies could be better equipped to spot bugs that impact a supply chain. SBOMs can also give security executives some peace of mind by answering these questions in light of new vulnerabilities, whether for software built in-house or acquired externally. Once utility companies are alerted to a vulnerability, with a SBOM they can better locate the code containing the issue and determine how to reduce downtime and how quickly they can patch it to restore services.

NERC-CIP & IEC 62443

The North American Electric Reliability Corporation (NERC)[4], a non-for-profit international regulatory authority whose mission is to assure the effective and efficient reduction of risks to the reliability and security of the electric grid. The newest version of NERC standards is called CIP (Critical Infrastructure Protection). These standards are used to secure bulk electric systems and apply directly to the utilities sector. IEC 62443 is an international series of standards for Industrial communication networks, IT security for networks and systems. The IEC standard is divided into different sections and describes both technical and process-related aspects of industrial cybersecurity, which also applies to utilities infrastructure.[5] Cybeats can support various aspects of enterprise cybersecurity, and for both of these applicable compliance requirements.

Utility Industry Market Size

The U.S. Utilities market size was USD $640 Billion in 2021 and CAD $60 Billion in Canada during the same time period. The global utilities market is on pace to be USD $4.5 trillion in 2021, with varying degrees of software mandates and requirements across different country's borders.[6] As the energy and utilities sectors face technological change across these sub-sectors, so are the mandated requirements that will include software supply chain and SBOM, which Cybeats products directly address the mandated technological changes and software supply chain security faced by the energy and utility sectors.[7]

The U.S. power system has evolved into a highly complex system with 3,300 utilities that work together to deliver power through 200,000 miles of high-voltage transmission lines. There are 55,000 substations and 5.5 million miles of distribution lines that bring power to millions of homes and businesses. Any of the system's principal elements including power generation, transmission, or distribution could be targeted and potentially shut down due to a cyberattack.[8]

Cyber Attacks on Utility Sector

Canadian Center for Cybersecurity wrote that cybercriminals would likely be capable of targeting the Canadian electricity sector for extortion within the next three years.[9] Studies have found that 56% of Utilities have faced a cyber-attack in the past year.[10] Whether a cyber attack on a power grid leading to a black-out on Christmas Eve[11], or attacks on water supply in L.A. and Portland, there have been severe disturbances to utility companies recently. "Water and Power sectors are shockingly vulnerable to cyberattacks," wrote Bloomberg.[12] Cybersecurity experts agree that at some point in the near future cyber criminals based in other countries could shutdown at least some portions of the U.S. power grid, if not the entire grid.[13]

Recent Cybersecurity News, M&A

Akamai acquired cybersecurity firm Guardicore for $600 million USD.[14] Cybersecurity Ventures predicts global cybercrime damages will cost the world $6 trillion annually by 2021, up from $3 trillion in 2015. Global cybersecurity spending is expected to reach $1 trillion cumulatively for the 5-year period from 2017 to 2021.[15]

RECENT NEWS: Announced Cybeats products that address the Electric Vehicles and Charging stations security markets : https://bit.ly/3BfEpu5

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

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. Relay recently acquired Cybeats Technologies, a platform which offers a holistic approach to cybersecurity and addresses the $73 billion IoT security market through their Software Bill of Materials and microagent solution. Cybeats provides real-time cybersecurity for connected devices, critical infrastructure, automotive, medical and IoT (Internet of Things) sectors.

The Company held a Special Meeting to approve a Name Change on September 20, 2021 as the Company's core competencies and product offerings have organically grown beyond the medical device industry, and this expansion into new industries and businesses will be reflected in the Name Change. The Company's new name will more aptly and effectively communicate the business and its commercial verticals.

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.utilitydive.com/news/software-bill-of-materials-sbom-biden-executive-order-supply-chain/606947/

[2] https://www.utilitydive.com/news/whats-in-your-software-federal-initiative-targets-frequently-overlooked-e/595820/

[3] https://www.utilitydive.com/news/whats-in-your-software-federal-initiative-targets-frequently-overlooked-e/595820/

[4] https://www.nerc.com/AboutNERC/Pages/default.aspx

[5] https://en.wikipedia.org/wiki/IEC_62443

[6] https://www.globenewswire.com/en/news-release/2021/03/15/2192582/28124/en/Global-Utilities-Market-Report-2021-to-2030-COVID-19-Impact-and-Recovery.html

[7] https://www.ibisworld.com/industry-statistics/market-size/utilities-united-states/

[8] https://www.cfr.org/report/cyberattack-us-power-grid

[9] https://cyber.gc.ca/en/guidance/cyber-threat-bulletin-cyber-threat-canadas-electricity-sector

[10] https://dailyenergyinsider.com/infrastructure/22281-survey-56-percent-of-utilities-have-faced-a-cyberattack-in-the-last-year/

[11] https://www.forbes.com/sites/jimmagill/2021/07/24/experts-say-cyberattacks-likely-to-result-in-blackouts-in-us/?sh=7a8a9622372d

[12] https://www.bloomberg.com/news/articles/2021-06-12/u-s-water-and-power-are-shockingly-vulnerable-to-cyberhacks

[13] https://www.forbes.com/sites/jimmagill/2021/07/24/experts-say-cyberattacks-likely-to-result-in-blackouts-in-us/?sh=72158622372d

[14] https://cybersecurityventures.com/mergers-and-acquisitions-report/

[15] https://cybersecurityventures.com/

Relay Medical.

To view the source version of this press release, please visit https://www.newsfilecorp.com/release/99070