Contact: 647-872-9982
Toll-free/Fax: 1-844-247-6633

Email: info@relaymedical.com
65 International Blvd. Suite 202
Etobicoke, Ontario M9W 6L9

Cybeats Addresses the Electric Vehicle Security and Charging Station Markets; Relay Comments on Mandated Software Requirements for EV Manufacturing and Infrastructure via SBOM

TORONTO, September 29, 2021 – Relay Medical Corp. (**"Relay"** or the **"Company"**) (**CSE: RELA, OTCQB: RYMDF, Frankfurt: EIY2**) reports on the addressable markets of electric vehicles (**"EV"**) connected security, including connected vehicle supply chain, software compliance and the associated EV charging infrastructure security markets. Cybeats is actively engaged and targeting these sectors as its products manage EV supply chain risk, help satisfy software compliance requirements, and most importantly support keeping people safe by securing connected vehicles and infrastructure.

Connected vehicles and the supply chain for various auto parts represent a new and critical cyber-attack opportunity for malicious hackers. A myriad of components go into electric vehicles, many of which are supplied from foreign countries which is a major concern for national security efforts to secure critical devices and infrastructure. As the connected EV supply chain becomes more autonomous and complex, the more EV manufacturers will be required to monitor and secure these vulnerable systems. Cybeats offers cybersecurity solutions for IoT connected devices, including electric vehicles, and throughout the product life cycle. EV and the associated sectors require extensive security investment and management, and Cybeats is poised to offer solutions.

"Software plays a critical role in the automotive industry and with it comes the need for effective cybersecurity solutions," **said Yoav Raiter, CEO, Relay.** *"Cybeats has strengthened its foundation in cybersecurity with platforms like the SBoM Studio™, enabling us to be even more prepared for the era of EV and connected cars. This is a sector that Cybeats has been pushing toward, as autonomous and connected cars become more prevalent. Cybeats expects to be a competitive force as it charges toward this rapidly growing and critical sector."*

Cybeats Offers Security for Electric Vehicles, Manufacturing and Charging Stations

Cybeats offers security solutions to multiple EV supply chains such as the components of a vehicle, manufacturing facilities and electric charging stations. Cybeats has expanded its cybersecurity product offering to include automated vulnerability management for EV and for automotive charging stations. OEMs can now mitigate risk exposure to regulatory violations, liability claims and negative impacts to brand equity, using the Cybeats cybersecurity platform.

EV's, along with most auto manufacturing, are assembled by OEMs making it necessary to assess, manage, and secure all components and supply chains and the connected infrastructure involved in manufacturing

Contact: 647-872-9982
Toll-free/Fax: 1-844-247-6633

Email: info@relaymedical.com
65 International Blvd. Suite 202
Etobicoke, Ontario M9W 6L9

EV. Cybeats SBOM Studio™ platform offers valuable Supply Chain Risk Management (SCRM)[1], which provides the infrastructure and tools to design, develop and manage secure software components across every process of designing and manufacturing an EV. Cybeats ensures industry regulations, standards, and company policies are monitored and enforced throughout the life cycle of the vehicle.

Through vulnerability management, compliance validation, incident response, continuous monitoring, automatic updates, and management reporting, Cybeats monitors and alerts manufacturers of cybersecurity risks automatically and continuously throughout the design and development stage. As opposed to commonly-used firewall security which fortifies the perimeter of a network, Cybeats continuously monitors the operational state of a device and its components, and provides actionable alerts and intelligence in real-time. With this, Cybeats capabilities differ from standard security solutions and the industry defines this as a Run-time Application Self-Protection (RASP)[2], which offers EV manufacturers a platform with the future of cybersecurity in mind.

EV Charging Station Vulnerabilities

A group of engineers from the Southwest Research Institute (SwRI) spearheaded a malicious attack on EV charging processes. The team performed three manipulations to see if the EV charging system was hackable as part of an automated cybersecurity research initiative. During the exercise, they were able to expose the charging process's vulnerabilities, which resulted in the EV not being able to charge properly.[3] "This was an initiative designed to identify potential threats in common charging hardware as we prepare for widespread adoption of electric vehicles in the coming decade," Austin Dodson, lead Research Engineer, SwRI. Additionally, U.K. cybersecurity company Pen Test Partners has identified several vulnerabilities in six home EV charging brands and a large public EV charging network.[4]

SBOM and the EV Supply Chain

The Biden Administration is accelerating EV infrastructure[5] and now requires a standard of transparency in the software supply chain via a SBOM for critical sectors.[6] Automobile software companies know that integrating SBOM's is not only integral to car security, but also required for regulatory compliance and

[1] https://www.cisco.com/c/en/us/products/security/supply-chain-risk-management.html
[2] https://en.wikipedia.org/wiki/Runtime_application_self-protection
[3] https://www.trendmicro.com/us/iot-security/news/6510
[4] https://techcrunch.com/2021/08/03/security-flaws-found-in-popular-ev-chargers/
[5] https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/22/fact-sheet-biden-administration-advances-electric-vehicle-charging-infrastructure/
[6] https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

Contact: 647-872-9982
Toll-free/Fax: 1-844-247-6633

Email: info@relaymedical.com
65 International Blvd. Suite 202
Etobicoke, Ontario M9W 6L9

critical for national defense. Integrating SBOM standards into the EV manufacturing and development pipeline is a clear and widespread directional move for the industry. The SBOM inclusion in the Biden Executive Order is meant to reduce risk to national security, and the private industry understands that this has costs and economic consequences. Either way, automobile manufacturers will require these connected vehicles to generate and maintain SBOM, for which Cybeats provides the necessary platform, tools and ongoing management.

An additional aspect of EV cybersecurity is to support firmware updates to cars, a process where many vulnerabilities can be identified and corrected to optimize security. EV charging stations are exposed to cyber-attacks as well, for example by hackers attempting to modify vulnerable software on internal components such as microprocessors or memory.[7]

Electric Vehicles & Charging Market

The global electric vehicle market was valued at USD $160 billion in 2019, and is projected to reach USD $800 billion by 2027, registering a CAGR of 22.6%. EV's will make up 85% of new car models by 2040.[8] The charging grid and infrastructure connects vehicles to the power grid, the payment management system, and a variety of service providers, and is designed to send and receive data. Electric vehicles and the associated charging infrastructure are therefore as vulnerable to suffering cyber threats as any other connected device.

The Electric Vehicle charging stations market is estimated to grow from $17 billion in 2021 to $110 billion in 2028 at a CAGR of 30.26%[9], with roughly 2 million charging stations in 2020 to over 30 million charging stations by 2027.[10]

On September 28, Ford Motors[11] announced that its battery supplier SK Innovation plans to invest more than $11.4 billion in new U.S. facilities that will create nearly 11,000 jobs to produce electric vehicles and batteries.[12] Before there was a concept of product liability for the automobile manufacturers, there was no concept of product liability. We are now experiencing this global change.

LG Invests in Automotive Cybersecurity

[7] https://www.dekra-product-safety.com/en/importance-cybersecurity-electric-vehicle-charging-stations
[8] https://autocrypt.io/solutions/ev-charging/
[9] https://www.fortunebusinessinsights.com/electric-vehicle-ev-charging-stations-market-102058
[10] https://www.marketsandmarkets.com/Market-Reports/electric-vehicle-supply-equipment-market-89574213.html
[11] https://www.ford.ca/
[12] https://www.cnbc.com/2021/09/27/ford-battery-supplier-to-spend-11point4-billion-to-build-new-us-plants.html

Contact: 647-872-9982
Toll-free/Fax: 1-844-247-6633

Email: info@relaymedical.com
65 International Blvd. Suite 202
Etobicoke, Ontario M9W 6L9

On September 23, LG[13] acquired a majority stake in Cybellum, an Israeli automotive cyber security risk assessment company, with a transaction valued at USD $240 million.[14] Cybellum detects and assesses vulnerabilities involved in connected vehicle services. Cybellum's technology, and LG's acquisition of it, underscore some significant trends in the world of connected cars and cybersecurity.[15]

RECENT NEWS: Relay recently addressed the revelation about the widely-used Hikvision[16], a Chinese state-owned surveillance and connected security camera manufacturer, whereby a critical vulnerability was discovered in more than 100 million connected devices currently operational in the market: https://bit.ly/3zFSVtp

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.

[13] https://www.lg.com/global/mobility/press-release-detail
[14] https://techcrunch.com/2021/09/22/lg-is-acquiring-automotive-cybersecurity-startup-cybellum-in-a-240m-deal/
[15] https://swsolutions.lge.com/solutions/connected-car
[16] https://us.hikvision.com/en

Contact: 647-872-9982
Toll-free/Fax: 1-844-247-6633

Email: info@relaymedical.com
65 International Blvd. Suite 202
Etobicoke, Ontario M9W 6L9

Office. 647-872-9982
TF. 1-844-247-6633
Media Inquiries: media@relaymedical.com
Investor Relations: investor.relations@relaymedical.com

Bernhard Langer
EU Investor Relations
Office. +49 (0) 177 774 2314
Email: blanger@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.