Relay Provides State of Cybersecurity Webinar Highlights About SBoM; Recording Posted on YouTube

TORONTO, Sept. 21, 2021 (GLOBE NEWSWIRE) -- Relay Medical Corp. ("**Relay**" or the "**Company**") (CSE: **RELA**, OTCQB: **RYMDF**, Frankfurt: **EIY2**) is pleased to share a recording of the recent "State of Cybersecurity Industry - The Roots of SBoM" webinar featuring key panelists Kate Stewart, Steve Springett, and Relay's VP of Strategy Chris Blask. The webinar is the second of many for Relay, the panelists came together to discuss key cybersecurity issues and the recent Biden Administration Executive Order (EO) on Improving Nationwide Cybersecurity and tasked the National Telecommunications and Information Administration (NTIA) to establish security standards including defining SBoMs.

Notable attendees include:

- Allan Friedman, previously the Director of Cybersecurity Initiatives at NTIA in the US Department of Commerce
- Tom Alrich, who is currently the Co-leader of the Energy Sector SBoM Proof of Concept at NTIA

Last week, Relay held a live webinar with three world class cybersecurity leaders Kate Stewart, Steve Springett and Chris Blask. Kate Stewart is the Vice President of Dependable Embedded Systems at The Linux Foundation. Kate is a renown innovator and leader in system software and application tools as well as one of the original founders of Software Package Data eXchange (SPDX). Alongside Steve Springett who is the Chair of CycloneDX SBoM Standard, Core Working Group, a global leader in Defensive Design, Programming and Automation. A returning panelist is Chris Blask, Vice President of Strategy at Relay and also a respected influencer, innovative co-creator of the Digital Bill of Materials (DBoM), and one of the first commercial firewall products. The panel was moderated by industry expert Evgeniy Kharam, co-host of the Security Architecture Podcast.

Influential people who attended were among the likes of Allan Friedman, who many consider to be the father of the SBoM concept as he introduced it to the NTIA, commented during the event "the 'roadmap to the attacker' argument!" when the panelists were asked the question 'Can SBoMs be used by adversaries for crafting an attack?' Allan Friedman is the now Senior Advisor and Strategist at the Cybersecurity and Infrastructure Security Agency, and was previously alongside President Joe Biden during the Executive Order[1] which included the implementation of SBoM.

Richard Brooks, Senior Consultant and Co-founder Reliable Energy Analytics LLC, commented "I love the community support from both SPDX and CycloneDX - this gives me reason to be optimistic for SBoM adoption going forward."

Tom Alrich, Co-leader, Energy Sector SBoM Proof of Concept at National Technology and Information Administration, US Dept. of Commerce, agreed in reply with "The healthcare proof of concept is still going on" when Chris Blask answered the question posed by the audience 'Is it important for medical devices and as well pharma?' Chris said "In the medical sector, there was a health care proof of concept that the department of commerce where the National Telecommunications and Information Center Administration (NTIA) worked alongside the community a year and a half ago to provide SBoMs and like any other critical infrastructure we would expect healthcare to move with the market or ahead… I imagine them to be an early adopter".

Steve Springett answered the question posed by Duncan Sparell, NTIA Software Component Transparency Working Group Member: "Admittedly many software projects don't yet have SBoMs, but some do. Can the speakers each share how many SBoMs already exist and give some examples of SBoMs that they are aware of?" Steve said, "There are a lot of nuances in regards to which projects would actually benefit from SBoMS. For example, the open Java Development Kit (JDK) is in the process of producing SBoMs and there are some other large library-type things that are Software Development Kit (SDK) projects that are also in the process of adopting them which is great. However when you start looking at individual libraries, does it make sense to have SBoMs for them? The reality is that when you reuse these components in your own application your dependency graph isn't fully resolved until your build life cycle. There is a lot less value in having SBoMs for those projects versus other projects where SBoMs are much more valuable."

The recording can be found on the Company's Youtube channel:
https://www.youtube.com/watch?v=jlWPPNuCZTQ&t=740s

Key Questions and Answers

Why do we need SBoM and what purpose does it serve? (Timestamp 2:42)

Kate Stewart answered: "Software Bill of Materials is a way of describing what is actually in your software and systems. It helps us to understand what pieces of software are running, the relationship between them, and which source files make up a component. These are all elements of a Software Bill of Material which we need in order to understand what the composition is. Once we have the transparency we can put automation in place to monitor them properly rather than manually."

What are some real-life examples for SBoM implementations? (Timestamp 5:31)

Steve Springett answered: “I think the number one use case in why SBoM is such a hot topic is being able to identify vulnerabilities in the software we use. This can include software such as a microservice, an IoT toaster, or any other software, regardless, it will include third-party components... We build software on these building blocks, especially since it is very expensive to build software from scratch. Therefore when we reuse components we take responsibility for code we did not write. This is why being able to accurately communicate what inventory there is, what the name and version of these components are, where you obtained that software from and potentially how it is built. These all allow you to perform different types of analysis on the pedigree and provenance, and being able to understand all the different types of modifications that were made. We are finally able to answer the questions of who wrote what, what went into this code, who made it, did I obtain this code from a country that my country does not agree with? It’s all these types of use cases that are really interesting on top of the vulnerability use case that is driving this SBoM adoption in the first place.”

Kate Stewart answered: “We ran into this with Amnesia 33 for instance, where we then had to go down to the source file level in order to understand if we were impacted by certain things. One of the things that excited me with automation is being able to communicate this information automatically which is the work that’s going on in the CSAF group (Common Security Advisory Framework) about vex and communicating key vulnerability."

Can SBoMs be used by adversaries for crafting an attack? (Timestamp 13:36)

Chris Blask answered: “The short answer is no, but it gets down to the very first question in security. If we start writing this information down, doesn’t that mean that all our enemies have all the information? To this question, every security person knows the answer is: ‘It depends.’ If you have software that is highly proprietary or vulnerable and you don’t want the bad guys or your competitors to get it, then you should be able to do that using existing business processes and available technologies. However the reality is when you look at each step that we’re looking to enhance and replicate with cyber means we find that businesses that are sharing this information, in most cases their mechanism for protecting that info are perhaps not adequate or fit for the purpose to share securely and perhaps in every case, their processes are not as secure as they thought they were.”

Evgeniy added, “So this may force the provider to have better libraries and better version and programming skills to not include potentially vulnerable libraries.”

Does SBoM help the buyer or product developer? (Timestamp 19:28)

Kate Stewart answered: “The short answer is both. For the buyer, it makes transparent the risk on certain elements, so you know exactly what you are buying. This also helps you to understand what the software product you're buying may depend on, and make a risk assessment and mitigation. When you are a supply chain manufacturer and you’re bundling and reselling components from third party sources in which you by default take ownership for... SBoMs are a very useful tool for risk analysis and helping maintain and create policies… Sometimes your legal team may say under certain licenses you can’t bring this component in because we know there are big risks associated with this and there are better solutions out there... Once we can share SBoMs in a way that everyone trusts similar to what is going on in DBoM then we can also have the automation happen for these corporations that are bringing components in from open sources and other vendors' policies to be standardized and checked against them... These things from a buyer's perspective can reduce risk."

Would SBoM help to eliminate or reduce software supply chain risks? (Timestamp: 32:50)

Chris Blask answered: "As SBoMs get adopted, businesses will be able to implement contract language that lets them establish terms under which information is made available. The classic example is contract language that says that a vendor will provide all or part of an SBoM if a vulnerability is noticed from a reputable source and is later issued, which may impact a product purchased. This brings several benefits. The cost of responding to a new vulnerability can be much less, and the time to resolve is much shorter. Importantly, vendors are able to more clearly express the control of their intellectual property and are better able to determine if that control has been compromised. Such information today is in large part shared ad hoc between individuals at partner businesses when using a variety of means such as email that can be expensive or impossible to track. These aspects of SBoMs and systems like Cybeats are necessary to support SBoM which will tend to reduce cost and improve efficiencies at multiple points and supply chains, providing competitive benefits for those businesses that adopt them early and well.”

Kate Stewart answered: “Being able to clearly articulate the software you got and be able to understand the implications of licensing as well as the implications if people found issues, answering the questions of should there be updates happening… These things are real and people need this capability, so making this easier for people is a big plus one.”

Where do you see SBoM in 5 years? (Timestamp 44:45)

Chris Blask answered: “In five years I see it built into everything… if you’re producing software and it is not creating SBoMs, you’re probably not involved in interesting things, and you're certainly not getting a lot of government RFP requests. If you’re a consumer operating in an enterprise in business or nation-state critical and you’re most likely not at the stage of learning how to use them, rather you are using them. It should be a part of your processes in procurement, security operations, and everything else.”

For future virtual events on Cybeats, subscribe to the Youtube channel:
https://www.youtube.com/channel/UCqtoSrovJvXcIJZz9uRxXbg

Recent News: Relay announces agreement with Unisys (NYSE: UIS)[2], a global IT solutions company, to market a combined solution for COVID-19 and biosecurity market needs: https://bit.ly/3AqDI0h

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.

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.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/
[2] https://www.nyse.com/quote/XNYS:UIS