Prepared Written / Oral Testimony of Bill Siegel, CEO and Co-Founder of Coveware Inc.

Committee on Homeland Security and Governmental Affairs

Rising Threats: Ransomware Attacks and Ransom Payments
Enabled by Cryptocurrency

Tuesday, June 7th 2022

Mr. Chairman, Ranking Member Portman, and members of the Committee, thank you for the opportunity to share Coveware's perspective on ransomware attacks and the role of cryptocurrency in ransom payments.

My testimony today is derived from Coveware's experience which spans thousands of ransomware incidents over the last few years. During a given incident, we interact with the victim of the attack, privacy attorneys, forensic investigators, restoration firms, cyber insurance companies, and the law enforcement agencies that investigate these attacks. Throughout the incident, we collect data first hand, and the aggregated learnings from this data, and our experience gives us a unique perspective on this problem. We collect and organize this data, because like any problem, you can't solve it until you understand it. The analogy we use is that you can't build safe cars without studying lots of car crashes first. In addition to analysis, our firm has voluntarily and proactively reported subsets of our data to law enforcement from every attack we have ever worked on since inception of our firm. This data is used by law enforcement to augment active investigations into the criminal groups that carry out these attacks.

We are grateful for the work that Chairman Peters, and Ranking Member Portman along with the committee staff have already completed in the publishing the staff report "CASE STUDIES IN RANSOMWARE ATTACKS ON AMERICAN COMPANIES" and the Majority Staff report "Use of Cryptocurrency in Ransomware Attacks, Available Data, and National Security Concerns."

Both of these reports highlight acute issues and we are grateful that this committee is collaborating with public and private industry and the

committee members are pursuing new legislation.

I'd like to quickly address the two primary areas of focus in these reports:

First with regards to cryptocurrency: Financially motivated cyber criminals almost universally denominate ransom demands in crypto-currency. The popularity of cryptocurrency with cyber criminals is rooted in the relative ease with which those criminals can protect ransom proceeds from seizure by law enforcement. The percentage of a ransom that finds its way to the cyber criminal's pockets is substantially higher when cryptocurrency is used vs. other currencies or stores of value. This is clear when looking at the recovery rates between two types of cyber crime, wire fraud and ransomware. If reported within 72 hours, illegitimate wires can typically be reversed and recovered. No such mechanism exists with crypto currency.

It is important to note that unlike financial theft, ransomware is much more akin to a kidnap and ransom incident. There are a number of variables that can prevent a ransom from being recovered once paid. Victims may not want their funds reclaimed out of fear that the criminals will not reciprocate with decryption keys, critical to restore an organization's business. Reclaiming a ransom also requires that the victim make a timely report to the correct branch of law enforcement. Moreover, for a trace and seizure to be successful the end destination of the cryptocurrency must be within the reach or western law enforcement. Most of the time, one or several of these variables inhibit a trace or seizure from even being started, let alone successful. It is also important to note that some form of currency, whether it be physical fiat, digital, or cryptocurrency has always been used for lots of different types of extortion. Ransomware existed before the advent of crypto-currency, and will persist if cryptocurrency were to ever disappear. As long as ransomware attacks are profitable to carry out against organizations with weak cyber security, cyber criminals will continue to proliferate these attacks. This brings us to the second topic of today's hearing, mandatory reporting.

Coveware has been vocal in our support for mandatory reporting for some time. Our hope is that reporting requirements will eventually be extended to

all victims of ransomware, not just organizations under the oversight of CISA.

As with any new law the efficacy lies in its implementation. This hearing is uniquely timed to allow policy makers to understand the dynamics of reporting, and ensure that final rules achieve the targeted impact. We believe there will be two primary impacts to mandatory reporting:

First, the US government will gain clarity on the scope of the problem. As was clearly documented in the Majority Staff Report, the variance between privately reported ransomware statistics and agency reported statistics is cavernous. Collecting accurate statistics is step number one and table stakes if new legislation or proposed solutions to solve this problem are to be taken seriously. Gaining clarity will allow agencies to more confidently resource their responses. We are encouraged to see that the Cyber Incident Reporting Act authored by Chairman Peters and Ranking Member Portman has begun to outline a clear path for reporting and unique agency responsibility.

The second impact will be in providing greater clarity on what to do about the problem. Gaining this clarity will hinge on WHAT information CISA collects, and IF CISA or other regulatory / law enforcement agencies are able to scalable digest the information reported to them. This new legislation has the potential to answer major questions, and enable CISA, the FBI, DHS and other agencies to make meaningful progress on this problem.

If not implemented correctly, however, the new legislation also has the potential to completely bury these agencies with unstructured data that cannot be parsed or analyzed at scale. This would render this new legislation completely ineffectual. Great care and focus should be applied to WHAT information is collected, and HOW this information is organized so that the velocity of analysis, recommendations and actions can achieve maximum efficacy.

Thank you very much Mr. Chairman. I look forward to answering the

Committee’s questions.