Testimony of

Megan H. Stifel
Executive Director, Americas
Global Cyber Alliance

Before the
United States House of Representatives
Committee on Homeland Security
Subcommittee on Cybersecurity, Infrastructure Protection, and Innovation

"Responding to Ransomware: Exploring Policy Solutions to a Cybersecurity Crisis"

May 5, 2021

Chairwoman Clarke, Ranking Member Garbarino, members of the Subcommittee on Cybersecurity, Infrastructure Protection, and Innovation, thank you for the opportunity to testify today on the growing threat ransomware poses to our homeland and national security.

My name is Megan Stifel, and I am the Executive Director, Americas, at the Global Cyber Alliance (GCA). GCA is an international nonprofit organization dedicated to providing practical solutions to reduce cybersecurity risk. I appear before you today as a co-chair of the Ransomware Task Force, convened by the Institute for Security and Technology, and comprised of over 50 organizations that gathered over the past 4 months to develop a comprehensive framework to reduce the risk of ransomware. Last week the Task Force published a report outlining its recommendations, including four goals and five priority recommendations, with a series of supporting actions constituting 48 total recommendations. The priority recommendations include the need for sustained, coordinated collective action among governments, industry, academia, and nonprofits to meaningfully reduce the ransomware threat.

I will focus my testimony today on three of these priority recommendations. First is the need for a coordinated, international diplomatic and law enforcement effort to prioritize ransomware, supported in the United States by a comprehensive whole-of-government strategy. Second is the need for enhanced information to support and enable this effort, including the development of a ransomware framework to help organizations better prepare for and respond to ransomware. And third is the establishment of Cyber Response and Recovery Funds and other assistance to support ransomware response and other cybersecurity activities.

As members of this subcommittee know well, the scale and scope of the ransomware challenge has grown exponentially over the past year. In 2019 the average ransomware payment was $43,593; by the end of 2020 it had quadrupled to $170,696.[1] Recent reports indicate some payments have stretched to the millions, while demands have reached the tens of millions.[2] But not just the size of ransom payments grew, so too did the number of organizations targeted, including hospitals and schools. In 2020, nearly 2,400 U.S.-based government, healthcare facilities, and schools were known to have been targeted with ransomware,[3] with the actual number affected potentially much higher. In addition to holding access to data hostage, ransomware actors are now threatening to publish data they have obtained from the victim's networks. According to Coveware, in the third quarter of 2020, 50% of ransomware attacks involved a threat to release data. That figure rose to 70% in the fourth quarter of 2020. Ransomware is plain and simple 21st century extortion.

[1] Coveware, "Ransomware Payments Fall as Fewer Companies Pay Data Exfiltration Extortion Demands," February 1, 2021, available at: https://www.coveware.com/blog/ransomware-marketplace-report-q4-2020.
[2] CNBC, "The extortion economy: Inside the shadowy world of ransomware payouts," April 6, 2021, available at: https://www.cnbc.com/2021/04/06/the-extortion-economy-inside-the-shadowy-world-of-ransomware-payouts.html.
[3] Emsisoft Malware Lab, "The State of Ransomware in the US: Report and Statistics 2020," January 18, 2021, available at: https://blog.emsisoft.com/en/37314/the-state-of-ransomware-in-the-us-report-and-statistics-2020/.

These figures illustrate that in just a few years ransomware has grown from a nuisance to a national security threat. And it is not just a problem for the United States. Organizations around the world have been targeted by ransomware.[4] As has also been well established, these threat actors operate from safe havens, countries whose governments are mostly unwilling as well as unable to support efforts to bring them to justice. Given the size of this threat, reducing its impact in one country is not possible without the assistance of others. Likewise, even if the United States and partner nations reduce ransomware in their own jurisdictions, without significantly limiting this threat at scale, there is little guarantee it will not simply emerge elsewhere, presenting an ongoing risk to the global community.

An International, Collaborative Effort Must Form to Reduce the Ransomware Threat

The Ransomware Task Force convened to address this growing international challenge. The breadth of the challenge informed the Task Force's first priority recommendation. Specifically, coordinated international diplomatic and enforcement efforts must make clear that ransomware is an international national security and law enforcement priority and that an international coalition should be developed to combat it. Governments should also develop a comprehensive, resourced strategy that uses both carrots and sticks to reduce the number of countries providing safe havens. In doing so, governments can build on the 2020 G7 finance minister's statement in further signaling publicly the urgency of this threat. But as the Task Force's other recommendations make clear, governments must also work collaboratively among themselves and with the private sector to share information, jointly investigate, and bring these actors to justice or otherwise eliminate their ability to operate with impunity.

For the United States, the Task Force recommends that this collective and collaborative action be driven by a whole-of-government strategy, led by the White House. Such a strategy should also include a Joint Ransomware Task Force to coordinate an ongoing, nationwide campaign against ransomware and identify and pursue opportunities for international cooperation. This joint interagency task force should be empowered at the appropriate levels to use all instruments of national power, and it should prioritize ransomware threats to critical infrastructure. In conducting its work, the interagency task force should also collaborate closely with relevant private-sector organizations that can help defend against and disrupt ransomware operations, such as security vendors, platform providers, information sharing and analysis organizations, and cybersecurity nonprofits.

The Task Force further recommends the development of a Ransomware Threat Focus Hub that can also support existing, informal efforts. The Hub can serve as a central, organizing node for informal networks and collaboration of a sustained public-private anti-ransomware campaign. In addition, to support the Hub's and its participants' ability to disrupt the ransomware lifecycle, the Task Force also recommends that the Departments of Justice and Homeland Security provide further clarity on the scope of defensive measures entities may undertake pursuant to the Cybersecurity Information Sharing Act of 2015.

[4] Sophos, "The State of Ransomware 2020," May 2020, available at: https://www.sophos.com/en-us/medialibrary/Gated-Assets/white-papers/sophos-the-state-of-ransomware-2020-wp.pdf.

The Scope and Quality of Information About Ransomware Must Improve

In order to develop and support this international strategy and its domestic elements, and through such a strategy eliminate safe havens, members of the Task Force believe that better information is necessary to enable this collective action. It is important to emphasize that this is not just more information sharing of cyber threat indicators, or indicators of compromise (IOCs), as they are also called. Both the scope and quality of information must improve. For example, IOCs should be tied to ransomware incidents, and this information must get into the hands of those who can use it - within the government as well as outside it. IOCs also need to be supplemented with additional information about ransomware incidents, including payments.

Due to the limited and inconsistent nature of information about ransomware incidents, the Ransomware Task Force also recommends that national governments encourage organizations that experience a ransomware attack to voluntarily report the incident. Furthermore, the Task Force recommends that should a victim elect to pay the ransom they be required to share details with the government in advance of such payment. At a minimum, the notification should include the ransom date, demand amount, and payment instructions (e.g., wallet number and transaction hashes). Gathering and analyzing this information is essential not just for law enforcement but also for incident responders and insurers, who can deploy additional analytic tools that may help cybersecurity firms prevent the next incident as well as allow insurers to pursue payment recovery, including through subrogation.

This information is necessary but insufficient to fully combat this threat. Organizations, both their leadership as well as those in operational roles, need to better understand that ransomware is a real and relevant threat and have better guidance on how to prioritize mitigation efforts given limited resources. To address this knowledge gap, the Task Force recommends that a framework be developed to help organizations better prepare for and respond to ransomware attacks, together with materials to support framework implementation such as toolkits and other how-to resources. Importantly, this framework should include customized recommendations based on each organization's current capacity to implement the recommendations. Following the success of the Cybersecurity Framework, the Task Force recommends that the National Institute of Standards and Technology convene an effort to develop this ransomware framework, in collaboration with international counterparts. The development of toolkits and other how-to materials are a necessary complement to ensure widespread adoption of the ransomware framework. GCA (and other organizations, I am sure) is ready to add such guidance to our existing resources to assist organizations in reducing their ransomware risk.[5]

[5] Global Cyber Alliance Blog, "Combatting Ransomware: A Call to Action," April 29, 2021, available at: https://www.globalcyberalliance.org/combatting-ransomware-a-call-to-action/.

Establishing Response and Recovery Funds and Expanding Grant Availability Can Support Victims and Disrupt the Ransomware Business Model

Resources for implementation are essential to the success of the ransomware framework and through it the disruption of the ransomware business model. To address this need, the Task Force recommends that governments establish Response and Recovery Funds. These funds should cover the cost, for example, of restoring systems for victims that serve essential functions including local governments as well as critical national functions. The Task Force believes that the availability of these funds will help reduce the number of victims electing to pay the ransom demand. As an incentive for organizations to invest in cybersecurity, governments could consider requirements to access the fund, such as demonstrating use of the ransomware framework to ensure a commitment to a baseline level of cybersecurity.

In addition, the Task Force recommends that more grant funding be available to use for cybersecurity. For example, Homeland Security Preparedness Grants could be expanded to address cybersecurity threats. Additional grants, along the lines established by the Help America Vote Act, could also be made available to states through which they could manage delivery of funds to municipalities. Not only would these investments reduce cybersecurity risks, they will also enhance state, local, tribal, and territorial resilience as upgrading software and hardware are often the most cost-effective security investments organizations can make. As with Response and Recovery Funds, access to these grants could be conditioned upon demonstrated alignment with the ransomware framework following its development. Elements of the State and Local Cybersecurity Improvements Act, which passed the House of Representatives last session, could serve as a baseline effort to address these recommendations.

On a personal note, I'd like to emphasize the importance of these grants. A dollar spent to prevent a crime will be more effective than a dollar spent to recover from it. Moreover, some grant funding should be focused on prevention mechanisms that can be used by many and work at scale rather than requiring every grantee to reinvent the wheel.

Conclusion

Combating ransomware is important because it is threatening large sections of the U.S. and global economy including healthcare services and schools. Left unchecked, its rapid growth is threatening national security, and payments associated with it are supporting a number of societal harms including human trafficking and the development of weapons of mass destruction. To combat this challenge, the Ransomware Task Force believes that the previously described recommendations together with other actions detailed in its report will, when implemented collectively, significantly reduce ransomware in the coming years.

In cybersecurity it is not often the case that one player can also fulfill another's role - we each have unique roles and bring unique capabilities. The Task Force offered a range of actions that could be taken building upon these unique capabilities, including with nonprofit resources, to stem this burgeoning threat. In closing, I want to highlight the essential role nonprofits played in the development of the Task Force's recommendations and that they can play in its implementation. Nonprofits may develop policy recommendations, support information sharing, and in the case of GCA, provide guidance on the implementation of established cybersecurity best practices including to combat ransomware. Nonprofits depend on contributions from a range of stakeholders to fulfill their unique and important roles. What is most important is that more action be taken by all stakeholders.

Thank you again for the opportunity to testify today. I welcome your questions and comments.