Institute for SECURITY + TECHNOLOGY

securityandtechnology.org

Testimony of

Megan H. Stifel
Chief Strategy Officer
Institute for Security and Technology

Before the
United States Senate
Committee on Homeland Security

“Rising Threats: Ransomware Attacks and Ransom Payments, Enabled by Cryptocurrency”

June 7, 2022

Chairman Peters, Ranking Member Portman, distinguished members of the Committee, thank you for the opportunity to testify about the importance of relevant information related to ransomware attacks and associated payments in combating the ongoing ransomware scourge.

My name is Megan Stifel, and I serve as the Chief Strategy Officer at the Institute for Security and Technology, or IST. IST is a Bay Area-based non-profit organization focused on staying ahead of security challenges resulting from our increasing dependence on technology. Our current work focuses on nuclear command and control, artificial intelligence, digital cognition and democracy, and, most relevant for today's purposes, information security.

Early last year, in response to the growing threat posed by the escalating rise in ransomware incidents targeting critical infrastructure, IST convened the Ransomware Task Force and I had the privilege of serving as a co-chair. The Ransomware Task Force included participants from industry, academia, civil society, and governments, including the United States, the United Kingdom, and Canada, as well as multilateral organizations such as Europol. In total, 60 plus organizations participated, including the organizations represented by my fellow witnesses. In a span of four months this coalition of stakeholders worked across four working groups, and examined measures to help better deter, disrupt, prepare, and respond to ransomware.

In April 2021, we published a report outlining the recommendations, including four goals and five priority recommendations, with a series of supporting actions constituting 48 total recommendations.[1] The priority recommendations included the need for sustained, coordinated collective action, led by the United States, among governments, industry, academia, and nonprofits to meaningfully reduce the ransomware threat; an intelligence-driven anti-ransomware campaign, coordinated by the White House, including the capability necessary to support operational collaboration with industry; the establishment of ransomware response and recovery funds, a framework for preparation, and mandated reporting of ransom payments; as well as closer regulation of the cryptocurrency sector that enables ransomware crime, including through compliance with existing tools designed to reduce illicit payments, e.g., Know Your Customer, Anti-Money Laundering, and Combatting Financing of Terrorism rules and regulations.

Just days after the report's publication, several high profile ransomware attacks occurred, leading to the disruption of fuel and meat product distribution as well as the delivery of healthcare. These were not the first incidents to target critical infrastructure, but, reflecting on them one year on, together they formed a pivotal moment. Since these incidents, significant progress has been made in countering ransomware. Much of the progress aligns with the Task Force's recommendations. And yet much more work remains.

[1] Institute for Security and Technology, Combating Ransomware, A Comprehensive Framework for Action, April 2021. https://securityandtechnology.org/wp-content/uploads/2021/09/IST-Ransomware-Task-Force-Report.pdf.

I will focus my testimony today on the Task Force's recommendations related to information about ransomware incidents, especially payments, in helping government and industry effectively combat ransomware. I will highlight where we have observed progress, and what remains in order to put ransomware actors on their heels for good.

Before I address the essential role of information in the ransomware lifecycle, I must pause to emphasize that ransomware is a symptom of a broader problem. That problem originated decades ago through a confluence of factors, all of which must be addressed to put a significant dent not just in ransomware-related cybercrime, but in most aspects of cybersecurity risk and resulting cybercrime.

Ransomware is 21st century extortion, but extortion is not a 21st century invention. New forms of extortionware are emerging. Thus, in examining collective measures by industry and government to combat ransomware, one of today's most significant cyber risks, we are not just targeting today, we are working to better secure tomorrow against whatever these criminals and other actors turn to next.

The Essential Role of Information in Order to Effectively Combat Ransomware

In my testimony last year before the House of Representatives Committee on Homeland Security, Subcommittee on Cybersecurity, Infrastructure Protection, and Innovation, I noted the Task Force's recommendation that the scope and quality of information about ransomware incidents must improve.[2] The need for better quality and greater information is manifold. Higher quality information can better equip governments and other stakeholders in developing the international strategy the Task Force called for to reduce ransomware on a global scale. It can provide more detailed evidence to support a range of measures that can be brought to bear in order to reduce the ability of these actors to operate from safe havens, to include sanctions on a range of infrastructure used to carry out their criminal activities. More detailed information can also enable diplomatic, law enforcement, and other instruments of national power. Of perhaps equal importance, higher quality information can better inform the private sector's ability to protect its and its customers' rights and property as well as enhance its capacity to collaborate with the government in combating ransomware and other cyber crimes.

As the Task Force noted in the April 2021 report, "improving the quality and volume of ransomware information would enable better deterrence, enhance preparedness, and inform disruption activities." It recommended several actions to support this objective. The actions included establishing a Ransomware Incident Response Network, creating a standard format for ransomware incident reporting, encouraging organizations to report ransomware incidents, and

[2] Megan Stifel, Testimony before the Subcommittee on Cybersecurity, Infrastructure Protection, and Innovation, May 2021. https://homeland.house.gov/imo/media/doc/2021-05-05-CIPI-HRG-Testimony-Stifel.pdf.

requiring organizations and incident response entities to share ransomware payment information with a national government prior to payment.

As I will describe in greater detail momentarily, through collaboration between industry and government, including several bills initiated or supported by this Committee, over the past year progress has been made in the fight against ransomware. Still, as the available information makes clear, more must be done.

Since ransomware is a criminal endeavor to extract financial gain, one of the most effective tools in combating it is to follow the money. Information—shared through voluntary and mandatory incident reporting, including of ransom payments—is this tool's lifeblood. Yet to this day we have not found an adequate incentive structure to meaningfully empower this capability.

As depicted in the attached ransomware payment diagram, ransom payments usually originate in fiat currency, which is then converted to cryptocurrency and moved from the victim's cryptocurrency wallet into the wallet controlled by the ransomware attacker. The first steps in this process, depicted on the left side of the diagram, are carried out largely through regulated entities. However, after the payment moves into the suspicious wallet, it can become increasingly difficult to track as it is laundered, exchanged, and cashed out to fiat currency. Information collected from victims about the size of the ransom and cryptocurrency transaction, the type of cryptocurrency used, the wallet address to which the payment was transferred, the Internet Protocol (IP) address(es) involved, and the transaction hash of the payment can enable law enforcement and blockchain analysts to better track payments through the entire cryptocurrency killchain. As this diagram suggests, a range of organizations may have information that can enable public and private sector entities to follow the money.
Today, however, there are only partial views spread across many stakeholders without a common process or pathway to stitch the pieces together.

Currently, the Cybersecurity and Infrastructure Security Agency (CISA), the Financial Crimes Enforcement Network (FinCEN), and the Federal Bureau of Investigation (FBI) collect varying aspects of this information through their individual reporting processes. However, a number of challenges remain with the current reporting pathways. Foremost among these challenges is inconsistency in the information requested. First, the FBI's Internet Crime Complaint Center (IC3) form, FinCEN's Suspicious Activity Report (SAR) form, and CISA's reporting process all ask for different information. For example:

- Account numbers are included in the IC3 and SAR forms, but not CISA's.
- IP addresses are required by the IC3 reporting form, but not by CISA or the SAR form.
- Only the IC3 and SAR forms ask for data about the perpetrators of the incident.

These differing data points highlight the need for a more streamlined approach to incident reporting. With multiple agencies collecting different information, it is highly likely that each agency will have a different picture of the attack, and the relevant steps needed to help the victim and prevent the next attack.

Ultimately, there should be harmony among government reporting avenues. This would ease confusion among victims, and streamline the collection and analysis of attack information. A common reporting format, which the Task Force recommended, would significantly assist this effort, and is something that we at IST, together with members of the Task Force, are working to develop.

The Cyber Incident Reporting for Critical Infrastructure Act will address aspects of this challenge, however, the need for consistency across reporting pathways is more immediate. It is especially critical while the rulemaking process is underway. It is also essential regardless of the rulemaking process, given the narrow scope of entities that will likely be required to report pursuant to it or share voluntarily under it.

Second, and compounding this problem, the extent of information sharing between these agencies remains unclear. The Committee's reports offer examples of information silos among agencies. For example, it is only recently the case, under the Cyber Incident Reporting for Critical Infrastructure Act, that CISA is required to share all incident reports it receives with the FBI. This type of information sharing will better position the FBI to investigate those responsible for ransomware attacks, while also allowing CISA to provide the technical assistance victims need to recover.

To meet the risks of tomorrow, information gathered must be useful and it must be appropriately disseminated within a meaningful period of time. It is also important to note that the same information may be of different value depending on an agency's or organization's mission. Within this same spectrum of challenges, it is also important to recall the emphasis placed by the Task Force on the need for disruptive capabilities of these payment channels: greater regulatory enforcement and reporting will help. The disruptive actions taken in the past year via coordinated action between departments and agencies to seize cryptocurrency assets could scale significantly if clear, concise, actionable information is made available to appropriate organizations as early as possible in the cryptocurrency killchain. When that information is provided days and weeks following an incident and/or payment, often the window for disruptive action may have already closed.

Recent Progress through Policy and Legislation

This Committee has led efforts to fund modernization of the nation's digital infrastructure, including through the passage of the Cyber Response and Recovery Act that established the Cyber Response and Recovery Fund, and the State and Local Cybersecurity Improvement Act, which were enacted in the Infrastructure Investment and Jobs Act. More recently, the Cyber Incident Reporting for Critical Infrastructure Act of 2022 requires reporting of incidents and payments for organizations identified through the ongoing rulemaking process. These funds, and the information ultimately provided pursuant to the legislation, should enhance our collective ability to combat the ransomware risk.

The policy measures initiated by the Administration included several measures to clarify expectations for preparation and response for critical infrastructure,[34] create more alignment and whole-of-government focus on deterring, disrupting, and prosecuting ransomware actors,[5] while reducing opportunities for attackers to realize a payday.[6] In addition, the June 2021 Group of Seven (G7) Summit Communique outlined a commitment to *"urgently address the escalating shared threat from criminal ransomware networks"* and called on all states to *"urgently identify and disrupt ransomware criminal networks operating from within their borders, and hold those networks accountable for their actions."* [7] In October, the United States also hosted a meeting with government officials from 30 nations to launch the Counter Ransomware Initiative. This meeting resulted in a joint statement and pledge for follow up actions that proved the impact of an international coalition.[8]

This leadership at the executive level exemplified recognition of, and response to, ransomware as a threat to national security. The commitment to stabilization was a watershed moment, setting a tone for a deep focus and hard work on this critical issue from various governments, including members of the G7.

Legislation together with policy developments designed to help the government better organize itself and its interactions with industry has aligned with over 85 percent of the Task Force's recommendations. In May 2022, the RTF published a report summarizing the progress of the 48 recommendations published in its April 2021 report.[9] The progress report referenced analysis from Crowdstrike and Chainalysis that found an 82% increase in ransomware attacks between

[3] U.S. Department of Energy, Office of Cybersecurity, Energy Security, and Emergency Response, "Colonial Pipeline Cyber Incident." https://www.energy.gov/ceser/colonial-pipeline-cyber-incident.

[4] Biden, Joseph R., Executive Order on Improving the Nation's Cybersecurity, The White House, May 12, 2021. https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/.

[5] Monaco, Lisa, Memorandum for All Federal Prosecutors, "Guidance Regarding Investigations and Cases Related to Ransomware and Digital Extortion," U.S Department of Justice, June 3, 2021. https://www.justice.gov/opa/press-release/file/1402001/download

[6] U.S. Department of the Treasury, Office of Foreign Assets Control, "Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments," September 21, 2021. https://home.treasury.gov/system/files/126/ofac_ransomware_advisory.pdf.

[7] Carbis Bay G7 Summit Communiqué, "Our Shared Agenda for Global Action to Build Back Better," G7 UK 2021, June 13, 2021. https://www.g7uk.org/wp-content/uploads/2021/06/Carbis-Bay-G7-Summit-Communique-PDF-430KB-25-pages-3.pdf.

[8] Joint Statement of the Ministers and Representatives from the Counter Ransomware Initiative Meeting, The White House, October 2021. https://www.whitehouse.gov/briefing-room/statements-releases/2021/10/14/joint-statement-of-the-ministers-and-representatives-from-the-counter-ransomware-initiative-meeting-october-2021/.

[9] Institute for Security and Technology, "The Ransomware Task Force: One Year On," May 2022. https://securityandtechnology.org/wp-content/uploads/2022/05/rtf-progress-report-may22-1.pdf.

2020 and 2021 and a 70% increase in ransomware payments over that same period. The progress report also noted "while security cryptocurrency researchers are pointing to these increases continuing in 2022, law enforcement, governments and cyber insurers are seeing reports of ransomware incidents slow down or even decrease."

This dichotomy in the overall direction of ransomware incidents points to a much broader problem. The limited operational collaboration and scale of information-sharing among and between government agencies and private industry partners has inhibited cooperation on disruptive actions against criminals. While significant progress has been made over the past year, governments still need to do more to support the private sector. In particular, the lack of comprehensive information about ransomware attacks continues to frustrate the private sector's ability to protect itself, inform policy development, and help take collective action against ransomware actors.

No matter how effective we become at deterring, disrupting, and preventing ransomware attacks, some percentage of attacks will succeed nonetheless. Many of the RTF's recommendations were aimed at increasing the availability of information about ransomware attacks in terms of frequency, volume, and other characteristics. This information is not just helpful for establishing trends–it will support effective use of the funds and authorities the Committee supported. Further, developing a clear understanding of the threat is a critical element in designing productive incentive structures to address the broader issues of cyber risk giving rise to the current ransomware spree. More immediately, enhanced information can help encourage victims not to pay ransoms, increase cooperation between law enforcement and victims, and support organizations that have fallen victim to a ransomware attack.

Keeping up the Momentum, Encouraging Voluntary Action

Legislation has been a necessary early step, but it is not enough, for several reasons. First, the timeline under which the requirements will be implemented spans several years. CISA has up to two years after passage of the Act to issue the notice of proposed rulemaking, and another 18 months to issue the final rule. This timeline does not reflect the urgency of the threat at hand. As I noted above, compared with 2020, in 2021, observed ransomware incidents rose by 82% and known payments rose by 70%. Those increases topped the prior years' record breaking rises. This growth pattern suggests it will rise again in 2022 and beyond, yet it will be several years before the types of organizations required to report become known, and even longer before they must report.

In the meantime, it is essential to increase utilization of other tools that can help organizations reduce the ransomware risk, including redoubling efforts to improve cyber hygiene and increase voluntary reporting.

To support organizations in improving their hygiene, later this summer the Task Force will publish the Blueprint for Ransomware Defense. Over the past several months, members of the Task Force worked together to develop a clear, actionable framework for ransomware mitigation, response, and recovery. The Blueprint aims to equip small and medium sized enterprises (SMEs) in particular with the security controls known to be most effective in mitigating ransomware risk. Tools that can assist in implementing the control recommendations will accompany the Blueprint. For the Blueprint to be effective, collaboration with SMEs and the managed service and managed security service providers, together with other support organizations, is essential. Members of the Blueprint working group are actively engaging these organizations in order to develop a solid foundation upon which to publish these resources.

The Blueprint addresses the Task Force's recommendation to develop guidance to support these organizations' preparation and response. As noted in the Task Force's April 2021 report, better equipping these organizations is essential to reducing their risk, and can also facilitate their ability to report information. While SMEs are currently not subject to the mandatory reporting requirements, by expanding the types of organizations sharing information related to incidents, relevant stakeholders will have a more comprehensive picture of the threat and be better equipped to prevent similar such incidents as well as help leverage appropriate tools to identify the responsible actors.

Even if victims more consistently share and report information about the incidents they experience, the mechanisms to collect, analyze, and disseminate that information remain immature. The statistics cited above reflect this problem; at best, they are estimates from a particular company's or government agency's point of view. While aggregating these different reports can provide a general sense of the trends, policy decisions and priorities should be based on more reliable data. Unfortunately, efforts to improve information sharing about ransomware attacks have been slow, due to competing priorities, legal and regulatory restrictions, and other perceived downsides.

The data we have is largely knit together through collaborations among law enforcement, government agencies, insurers, and researchers, but even this patchwork view is incomplete and likely distorts our understanding of the real situation. The resulting picture fails to capture the scope, scale, and impact of ransomware attacks, making it hard to accurately interpret available and incomplete data to assess the efficacy of actions being taken. This situation should improve as reporting requirements come into effect, but that takes time that we do not have while the threat landscape continues to evolve.

The willingness of victims to report incidents is likely an additional factor contributing to the lack of coherence about the direction of attack trends. Security researchers and cryptocurrency analysts are monitoring attacker-side activity visible on the dark web. By contrast, law enforcement and insurers are reliant on organizations making reports, which they often prefer not to do, particularly as sanctions and other regulatory requirements increase. For researchers, one other element that is currently providing more visibility of attacks is the growing double extortion trend. Researchers are able to track criminal groups selling or leaking stolen data. Due to the historic lack of clear and consistent reporting, it is unclear whether increased reports of stolen data for sale on the dark web amount to more ransomware attacks, or simply more attacks that incorporate double extortion.

There are additional legislative opportunities that could encourage voluntary information sharing. One path forward is to leverage safe harbors for victims who engage in appropriate due diligence. For victims of ransomware attacks, decisions about whether or not to pay ransoms and report incidents are stressful and time constrained. Even when victims feel they have done their due diligence before making a payment, many organizations fear enforcement actions, reputational impact, and other delays caused by reporting incidents. Providing safe harbor for these victims, in exchange for a commitment to report the incident and cooperate with law enforcement for the duration of any resulting investigation, would provide a carrot in an environment full of sticks.

A second path forward could be to implement the Cyberspace Solarium Commission recommendation for the creation of a “joint collaborative environment.” The Commission recommended that this environment be established to share threat information across the federal government and the private sector. In addition to enabling the sharing and fusing of threat information, insights, and other relevant data, the environment could enhance opportunities for disruptive action.

As the Committee’s Majority and Minority reports have recently noted, ransomware became and remains a significant risk to critical infrastructure and thus to our national security. The actors are going to continue to press at the seams of our public-private collaboration. Now is the time to prioritize the urgency of action, equip organizations with better information to protect themselves and respond to the threat, and leverage our collective capabilities to be best positioned for the future.

Conclusion

Members of the Committee, thank you for the opportunity to participate in today’s hearing. As the convener of the Ransomware Task Force, IST appreciates this Committee’s leadership in combating ransomware and stands ready to continue to collaborate with you in the years ahead. I look forward to your questions.

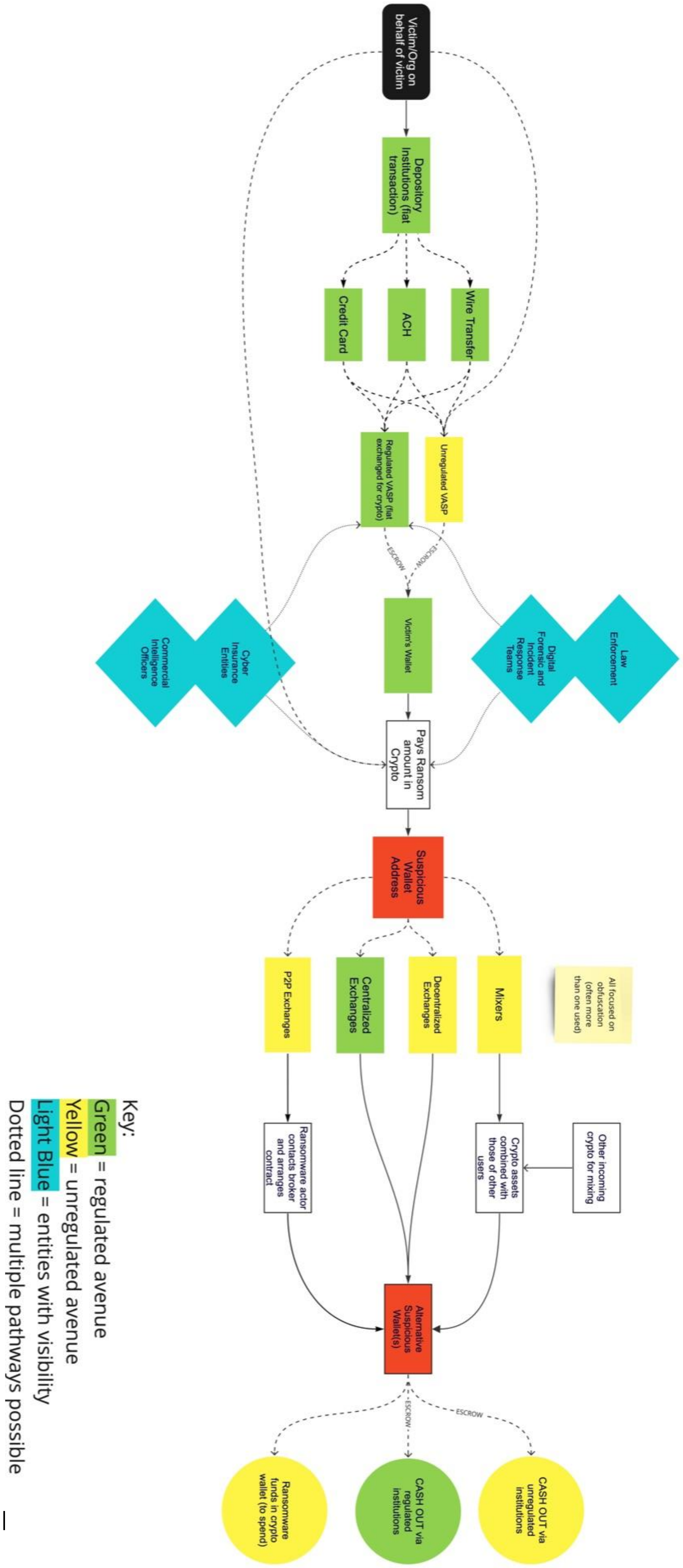
Victim/Org on behalf of victim
Depository Institutions (fiat transaction)
Wire Transfer
ACH
Credit Card
Unregulated VASP
Regulated VASP (fiat exchanged for crypto)
ESCROW
ESCROW
Law Enforcement
Digital Forensic and Incident Response Teams
Victim's Wallet
Cyber Insurance Entities
Commercial Intelligence Officers
Pays Ransom amount in Crypto
Suspicious Wallet Address
All focused on obfuscation (often more than one used)
Mixers
Decentralized Exchanges
Centralized Exchanges
P2P Exchanges
Other incoming crypto for mixing
Crypto assets combined with those of other users
Ransomware actor contacts broker and arranges contract
Alternative Suspicious Wallet(s)
ESCROW
ESCROW
CASH OUT via unregulated institutions
CASH OUT via regulated institutions
Ransomware funds in crypto wallet (to spend)
Key:
Green = regulated avenue
Yellow = unregulated avenue
Light Blue = entities with visibility
Dotted line = multiple pathways possible

Diagram Sources:

- https://www.fincen.gov/sites/default/files/advisory/2021-11-08/FinCEN%20Ransomware%20Advisory_FINAL_508_.pdf
- https://energycommerce.house.gov/sites/democrats.energycommerce.house.gov/files/documents/Witness%20Testimony_Walden_OI_2021.07.20.pdf
- http://ewfs.org/wp-content/uploads/2022/01/228_01.pdf
- https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/945411/NRA_2020_v1.2_FOR_PUBLICATION.pdf
- https://research.csiro.au/blockchainpatterns/general-patterns/blockchain-payment-patterns/escrow-2/