CSAW'21 Policy Competition

Background Paper for Ransomware

General Background

Spurred by the invention of cryptocurrencies, ransomware attacks have become increasingly sophisticated and can hold operations of businesses, volunteer organizations, or critical sectors hostage for hours to weeks unless a ransom is paid.[i] Data may be exfiltrated and posted online, ransoms may not be honored, and entire countries may feel the ramifications of a single ransomware attack.

Subtopic A: Ransomware Attacks on Critical Infrastructure

The Department of Homeland Security (DHS) has identified 16 critical infrastructure sectors all of which are intricately interconnected. Several critical infrastructure sectors such as telecom, finance, transportation, and healthcare are so vital that any destruction, disruption, or degradation of service could produce a nationally significant incident.[ii] These stakes make critical infrastructure prime targets for ransomware because the incentives to pay are high. For example, the Covid-19 pandemic created the conditions for a surge in ransomware attacks on the healthcare sector, with 1 in 3 health organizations worldwide reporting ransomware in 2020.[iii] Additionally, the US Southeast suffered gas shortages when Colonial Pipeline paused its natural gas distribution as part of its recovery from a ransomware event.[iv] Although hackers might target one company in one critical infrastructure sector, the vulnerabilities exploited are the same and disruptions could be felt throughout society.

Subtopic B: Payment Policies for Ransomware Attacks

If an organization pays a ransom, it has an 80% chance of being hit by ransomware again, often by the same hackers.[v] Businesses are incentivized to pay ransoms to protect personally identifiable information, intellectual property, or their reputation. In the United States, paying ransomware is legal so long as the hackers are not on a sanctions list.[vi] However, paid ransoms are used to fund adversarial governments, terrorist organizations, and the research and development for future ransomware attacks. Regulating cryptocurrency brokers, mandating ransomware reporting, and making ransom payments illegal are among many options being discussed to curb the payments funding ransomware attacks.

Main Issues

Competitors must choose **one** subtopic. They must address **at least one** bullet point within that subtopic, as listed below.

Subtopic A: Ransomware Attacks on Critical Infrastructure

- Responsibility of critical infrastructure operators in securing their networks from known vulnerabilities
- Role of law enforcement, military, and regulatory agencies in responding to and preventing ransomware attacks on critical infrastructure
- Incentives to make existing initiatives more effective at sharing information (for example, sectoral Information Sharing and Analysis Centers.)

Subtopic B: Payment Policies for Ransomware Attacks

- Current activities and practices that exist across the cryptocurrency ecosystem to make cashing out of ransomware more difficult
- International law enforcement and private-public cooperation in degrading and destroying digital infrastructure used in ransomware payments
- Incentivizing or regulating private-sector entities within the cryptocurrency ecosystem to prevent, monitor, or degrade ransomware payouts

What Needs to be Covered

Between the Policy Brief and Presentation, the bullet points below **must** be addressed.

For Sub-topic A: Ransomware Attacks on Critical Infrastructure only

- **Individual infrastructure sector: Pick 1 CISA sector for your policy memo and presentation response** and include a recent ransomware incident that impacted this critical infrastructure sector. How does your policy prevent an attack like this from happening again? What resources does that sector need to better prepare and prevent future ransomware attacks?
- **Federalism:** How does your policy address the significant divide between federal and state resources in dealing with hostile acts? How will local, state, and federal government activities be coordinated for maximum efficiency and effectiveness?

For both Sub-topics:

- **Funding:** What mechanisms will guarantee long-term funding? What tools, resources, infrastructure, or people need to be funded? How does funding account for expansion and updates?
- **Public-Private Cooperation:** How does your policy incentivize private sector cooperation? What weight should be accorded to private sector considerations during strategic decision making?
- **Short- & Long-Term Goals:** What is the timeframe for your policy? How does your policy assess short- and long-term success in accomplishing its objectives?

A note to CSAW Competitors

This brief is a starting point for your policies and ideas. It contains things you must address, but scope, definitions, and specific content will come from you. We encourage bold, creative policies that force deep thought and discussion. Leaders from academia, government, and private industry may see your work, and thus we encourage you to prioritize your policies by thinking through their practicality and implementation for a range of stakeholders. Please reach out to the CSAW committee at csaw-policy@nyu.edu with any questions.

Endnotes and Useful References

i. “History of Ransomware.” *CrowdStrike,* July 21, 2021. https://www.crowdstrike.com/cybersecurity-101/ransomware/history-of-ransomware/.

ii. “Critical Infrastructure Sectors.” *Cybersecurity and Infrastructure Security Agency*. https://www.cisa.gov/critical-infrastructure-sectors.

iii. Weiner, Stacy. “The growing threat of ransomware attacks on hospitals.” *Association of American Medical Colleges*, July 20, 2021. https://www.aamc.org/news-insight s/growing-threat-ransomware-attacks-hospitals.

iv. Kissane, Carolyn and Pano Yannakogeorgos “Hacking regrets: The Colonial Pipeline and lessons to be learned.” *The Hill*, May 12, 2021. https://thehill.com/opinion/cybersecurity/552944-hacking-regrets-the-colonial-pipeline-and-lessons-to-be-learned.

v. Sharma, Mayank. “Most ransomware victims who pay up just get attacked again.” *TechRadar*, June 16, 2021. https://www.techradar.com/news/most-ransomware-victims-who-pay-up-just-get-attacked-again.

vi. Marañon, Alvaro and Benjamin Wittes. “Ransomware Payments and the Law.” *Lawfare*, August 11, 2021. https://www.lawfareblog.com/ransomware-payments-and-law.

“Cyberspace Solarium Commission: Final Report.” *U.S. Cyberspace Solarium Commission*, March 2020. https://drive.google.com/file/d/1ryMCIL_dZ30QyjFqFkkf10MxIXJGT4yv/view.

“Securing Cyber Assets: Addressing Urgent Cyber Threats to Critical Infrastructure.” *U.S. Department of Homeland Security*, August 2017. https://www.cisa.gov/sites/default/files/publications/niac-securing-cyber-assets-final-report-508.pdf.

Wilson, Mike. “Why Paying Ransomware is Typically a Bad Idea and What You Can Do Instead.” *Forbes*, June 12, 2021. https://www.forbes.com/sites/forbestechcouncil/2021/07/12/why-paying-ransomware-is-typically-a-bad-idea-and-what-you-can-do-instead/?sh=2283e9201503.

By: Amanda Tobey and Rebecca Mader