National Council of ISACs Statement of Ransomware

Ransomware is a threat that the National Council of ISACs (NCI) and its member ISACs have been monitoring for years. With the increasing number of incidents of Ransomware, it is more important than ever that all enterprises take appropriate measures to protect themselves. Recently there have been some successes on the part of law enforcement and financial regulators as evidenced by indictments and the seizure of some ransom payments. The NCI calls upon businesses to redouble their efforts at cyber hygiene and references key resources to assist in network defense and pre-attack preparation. Additionally, the NCI is reiterating the importance of law enforcement and regulators across the globe to work with industry to identify, disrupt, and impose consequences on ransomware operators.

No sector is immune to Ransomware attacks. Ransomware can impact organizations of any size in any sector. However, there are steps organizations can take to reduce their risk and recover from a successful attack. These include:

- **Ensure devices are patched:** By deploying security patches organizations plug holes that attackers can exploit. To the extent possible, enable automatic updates. When not possible, ensure you have a risked-based patch management process.
- **End-user education:** Employees are an important component of an organization's cybersecurity. They should be trained to not click on links or documents they are not expecting and should be trained on how to identify suspicious emails.
- **Backup your data:** Backups ensure that you can recover from an attack. Since some ransomware variants target online backup systems, information should also be stored offline as well.
- **Engage with colleagues:** Engaging with industry peers is recognized as an effective practice in mitigating risks. If you are not a member of your sector specific ISAC, you should consider becoming a member or consider joining other information sharing forums.
- **Develop a response plan:** Companies should consider how they would respond if they became a victim of ransomware. Documenting a plan and practicing it, will help organizations respond more quickly.
- **Segment your networks:** To the extent possible, limit Internet connections to your operational technologies. If they must be connected to the Internet, ensure operational networks such as manufacturing, and production are segmented from business networks. This will limit risk to the operational networks and minimize risk to those operations if there is a disruption to the corporate networks.
- **Test Incident Response Plans:** If you already do not have a plan to guide your response to a cyber incident, you should build a plan with your security, legal, HR, and communications teams. If you have a plan in place, it should be tested regularly.

There are additional resources available to assist companies. These include:

- CISA Resources: Stop Ransomware
- NIST Preliminary Draft: Cybersecurity Framework Profile for Ransomware Risk Management
- U.S. Secret Service Report: Preparing for a Cyber Incident - A Guide to Ransomware v 1.0.pdf
- National Council of ISACs Report: Strengthening Cryptocurrency Regulation and Anti-Money Laundering Tools to Reduce the Impact of Ransomware
- Joint MS-ISAC and CISA Ransomware Guide: https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C.pdf
- White House Memo to Industry: What We Urge You To Do To Protect Against The Threat of Ransomware

In the fall of 2020, the NCI published a white paper titled “Strengthening Cryptocurrency Regulation and Anti-Money Laundering Tools to Reduce the Impact of Ransomware." This paper covered the exploding crime problem of extortionate ransomware operators. The paper called for international financial system regulators to enforce anti-money laundering laws uniformly across the world. In this same manner, we encourage law enforcement and government bodies to increase their cooperative efforts to address the ransomware problem and reduce the risk of a ransomware event on the operators of critical infrastructure and their supply chains.