DEPARTMENT OF THE ATTORNEY GENERAL

DAVID Y. IGE
GOVERNOR

CLARE E. CONNORS
ATTORNEY GENERAL

For Immediate Release
August 2, 2021

News Release 2021-48

Hawaii Attorney General Connors Joins Fellow Attorneys General in Alerting Businesses and Government Entities to Take Prompt Action to Protect Operations and Personal Information

HONOLULU – Following an unnerving increase in the frequency and scale of ransomware attacks across the globe—underscored by the massive attack on software company Kaseya on the brink of the July 4th holiday weekend—Attorney General Clare E. Connors joins a bi-partisan coalition of Attorneys General in urging businesses and government entities to immediately assess their current data security practices and take appropriate steps to protect operations and consumer data.

Ransomware is a form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Cybercriminals demand ransom in exchange for decryption, often threatening to sell or leak exfiltrated information if the ransom is not paid. Ransomware is a growing threat, generating billions of dollars in payments to cybercriminals and inflicting significant damage on businesses and government entities alike.

Earlier this month, REvil—a Russian-linked cybercrime gang—perpetrated the single largest global ransomware attack on record against the software company Kaseya. REvil's supply-chain attack on Kaseya's VSA software is believed to have infected thousands of client systems in at least 17 countries. A wide variety of businesses and public agencies were victims of the massive attack. REvil demanded $70 million in cryptocurrency in exchange for decrypting all affected machines—but in an unusual twist, by July 14, the group had disappeared from the Internet, along with sites where it directed its victims to negotiate and receive decryption tools. Last week, Kaseya announced that it had obtained a decryption key through a trusted third party and strongly denied having paid any ransom. This was REvil's second high-profile attack in recent weeks—having extorted $11 million from JBS Foods, the world's largest meat-processor, last month.

“Addressing cyber-threats and preventing cyber-breaches require vigilance by all organizations, particularly government and businesses,” Attorney General Connors said. “Up-to-date resources are readily available, however these prevention and response measures must be utilized and constantly updated to keep our systems safe against continually evolving threats.”

Attorney General Connors serves on the National Association of Attorneys’ General’s Internet Safety / Cyber Privacy and Security Committee, which serves as a resource for the attorney general community to discuss privacy issues. The Committee members’ joint advisory echoes a June 2, 2021 memo issued by Anne Neuberger, Deputy Assistant to the President and Deputy National Security Advisor for Cyber and Emerging Technology, titled “What We Urge You To Do To Protect Against The Threat of Ransomware.” The memo discusses the pressing threat that ransomware attacks pose to American businesses and government entities and recommends several best practices to respond to the threat and providing the following recommendations:

- **Implement the five best practices from the President’s Executive Order**: The President’s Executive Order on “Improving the Nation’s Cybersecurity” outlines five high-impact best practices that will significantly reduce the risk of a cyberattack: multifactor authentication (because passwords alone are routinely compromised), endpoint detection and response (to hunt for malicious activity on a network and block it), encryption (so if data is stolen, it is unusable) and a skilled, empowered security team (to patch rapidly, and share and incorporate threat information in your defenses).
- **Backup your data, system images, and configurations, regularly test them, and keep the backups offline**: Ensure that backups are regularly tested and that they are not connected to the business network, as many ransomware variants try to find and encrypt or delete accessible backups. Maintaining current backups offline is critical because if your network data is encrypted with ransomware, your organization can restore systems.
- **Update and patch systems promptly**: This includes maintaining the security of operating systems, applications, and firmware, in a timely manner. Consider using a centralized patch management system; use a risk-based assessment strategy to drive your patch management program.
- **Test your incident response plan**: There is nothing that shows the gaps in plans more than testing them. Run through some core questions and use those to build an incident response plan: Are you able to sustain business operations without access to certain systems? For how long? Would you turn off your manufacturing operations if business systems such as billing were offline?
- **Check your security team’s work**: Use a third-party penetration tester to test the security of your systems and your ability to defend against a sophisticated attack. Many ransomware criminals are aggressive and sophisticated and will find the equivalent of unlocked doors.
- **Segment your networks**: There has been a recent shift in ransomware attacks—from stealing data to disrupting operations. It is critically important that your corporate business functions and manufacturing/production operations are

> separated and that you carefully filter and limit internet access to operational networks, identify links between these networks, and develop workarounds or manual controls to ensure industrial control system (ICS) networks can be isolated and continue operating if your corporate network is compromised. Regularly test contingency plans such as manual controls so that safety critical functions can be maintained during a cyber incident.

All organizations face the threat of a ransomware attack. Guidance and resources from the U.S. Cybersecurity & Infrastructure Security Agency (CISA) on how to guard your organization against ransomware attacks can be found here. CISA and the Federal Bureau of Investigation (FBI) have also issued specific guidance for managed service providers (MSPs) and their customers affected by the Kaseya ransomware attack, discussed above. This guidance can be found here.

The National Institute of Standards and Technology (NIST) also provides guidelines and best practices for organizations to manage and reduce cybersecurity risk, which can be found here.

Victims of ransomware should report it immediately to CISA, a local FBI Field Office, or Secret Service Field Office. Victims should also file a report online through the Internet Crime Complaint Center (IC3).

# # # # #

Gary H. Yamashiroya
Special Assistant to the Attorney General
Department of the Attorney General
425 Queen Street
Honolulu, HI 96813