THE ALS GROUP

CISA/FBI Holiday Cyber Advisory

As air travel for the upcoming Thanksgiving weekend spiked to pre-pandemic levels and AAA estimates over 53 million people will hit the road this holiday, the Cybersecurity & Infrastructure Security Agency (CISA) and FBI issued an advisory yesterday, warning critical infrastructure partners that malicious cyber actors tend to strike during holiday weekends.

"Although neither CISA nor the FBI currently have identified any specific threats, recent 2021 trends show malicious cyber actors launching serious and impactful ransomware attacks during holidays and weekends."

This advisory, once again, emphasizes the importance of organizations being vigilant and take proactive measures to minimize the risk and impact of a potential cyber-attack, which based on 2021 trends seem to happen more during holidays when offices are closed.

One of the most effective measures is to evaluate their network security controls and ensure best practice mitigation strategies are in place.

Below are a few key best practices CISA and the FBI point out in the advisory:

- Identify IT security employees for weekends and holidays who would be available to surge during these times in the event of an incident or ransomware attack.
- Implement multi-factor authentication for remote access and administrative accounts.
- Mandate strong passwords and ensure they are not reused across multiple accounts.
- If you use remote desktop protocol (RDP) or any other potentially risky service, ensure it is secure and monitored.
- Remind employees not to click on suspicious links, and conduct exercises to raise awareness.

Individual users should heed this warning, especially while traveling:

- Be sure to keep the laptop, or mobile device is with them at all times
- Keep anti-virus software updated, and
- Limit use of public WiFi (airports, coffee shops, etc.).

While all of the above may help prevent a ransomware attack, having a comprehensive Disaster Recovery/Incident Response plan in place should your organization fall victim to one despite all of preventative measures will help minimize the financial impact such an attack will have.

There are several helpful documents that provide guidance such as the Ransomware Response Checklist in the CISA-MS-ISAC Joint Ransomware Guide, the Public Power Cyber Incident Response Playbook, and the new Federal Government Cybersecurity Incident and Vulnerability Response Playbooks.

If you have questions on how to manage your company's Cyber risk, or any other risk or insurance issues please contact Jon Edwards jedwards@thealsgroup.com.