AUGUST 30, 2022

IS YOUR ORGANIZATION PREPARED FOR A RANSOMWARE ATTACK?

Ransomware attacks on health care organizations have increased dramatically in 2022, costing organizations billions of dollars. Health care providers are being attacked by cybercriminals who encrypt their data and devices and demand monetary payment to make the data available again or prevent its further disclosure. As long as ransomware attacks remain lucrative, the frequency of such attacks are expected to continue to increase. **Is it time to assess the effectiveness of your cyber incident response plan?**

WHAT'S AT RISK?

Without a workable recovery plan in place and an understanding of potential vulnerabilities in your backups, you could be without working applications for weeks following a ransomware attack. Cyberattacks can also lead to permanent loss of critical data and data integrity, public release of sensitive information, government investigations and penalties and private litigation, including class actions.

Hall Render Advisory Services has the experience to help you identify gaps in your backup and recovery plans while evaluating ransomware attack preparedness.

Our team of advisors can equip your organization by:

- Analyzing your organization's preparedness for modern threats;
- Auditing and assessing your backup and recovery plans;
- Reviewing incident response processes; and
- Working with your business and IT teams to help them understand how simple changes can protect your organizations against ransomware attacks.

Contact: Acting swiftly to understand your organization's preparedness is critical in ensuring recovery from a ransomware incident. If you are ready to develop a robust cybersecurity program or enhance your existing cybersecurity program, let's chat. Advisory Services can work with your teams to identify practical, actionable solutions to prepare for and remediate the effects of a ransomware attack.