Security and Recovery Preparedness

Ransomware attacks on health care organizations have increased dramatically this year, costing these organizations billions of dollars. Health care providers are being attacked by cybercriminals who encrypt their data and devices and demand monetary payment or expose your data outside your organization or other types of disclosure. As long as ransomware attacks remain lucrative, the frequency of such attacks are expected to continue to increase.

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

WHAT YOU NEED TO KNOW

- Small to medium-sized health care organizations (e.g., hospitals, health clinics, ASCs, etc.) need to review their current security environment, focusing on protecting against ransomware attacks and other malicious cybersecurity threats, specifically through the lens of how backup systems are designed, clinical system recovery requirements, business operational application requirements including active directory and other operational tools.
- Traditional basic backup and recovery methodologies alone are not sufficient enough to recover from a major malware incident.
- Understanding how to safeguard PHI and PII from malware that is specifically designed to destroy a business's ability to recover from a backup now requires a new approach.
- Having a tested business continuity plan in understanding what is required to keep your business in operation during a major malware incident is critical.

CONNECT WITH US

Mark Swearingen
Attorney
mswearingen@hallrender.com

Melissa Markey
Attorney
mmarkey@hallrender.com

Dan Cumberland
Principal Advisor
dcumberland@hallrenderas.com

WHY HALL RENDER ADVISORY SERVICES?

Hall Render Advisory Services has the experience to help identify security gaps in your backup and recovery plans while also evaluating your ability to manage your operations if you are attacked by ransomware.

Our team of advisors can equip your organization by:

- Assessing your Business Continuity Plan for your organization's preparedness to keep systems operational from today's security threats;
- Auditing and assessing your backup and recovery plans;
- Testing your incident response plan; and
- Developing a Business Continuity Plan or Incident Response Plan you can test, if you don't have one.

LET'S GET STARTED

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

Last Updated on January 31, 2024