OCTOBER 19, 2021

CRITICAL ACCESS HOSPITALS: BRACE FOR CYBER-INSURANCE INCREASES

The health care industry has experienced significant increases in cyber-attacks such as ransomware the past few years. One segment of the industry that may be impacted especially hard by these increased attacks is Critical Access Hospitals ("CAHs"). Due to the increasing number of cyber-attacks, insurance underwriting practices are shifting. Instead of virtually rubberstamping each application for insurance, underwriters are now subjecting insurance applications to greater scrutiny, performing stronger risk analyses and rejecting more claims. Not surprisingly, the increase in cyber-attacks has resulted in significant increases in the cost of cyber-insurance.

Cyber-insurance underwriters want more certainty. They want more certainty that the insured is as best as possible a low risk for attack. They want their insureds to be prepared for and be resilient to a cyber-attack. They want their insureds to focus on preventing ransomware attacks, funds transfer fraud and business email compromise, which account for 87% of claims paid under cyber-insurance coverage.

In order to obtain these goals, cyber-insurance underwriters will review an organization's anti-phishing safeguards. Does the organization pre-screen emails for potentially malicious attachments and links? Does the organization have the capability to automatically evaluate attachments to determine if they are malicious prior to delivery? Does the organization publish and distribute written policies and procedures regarding computer and information security to its workforce members? Are workforce members provided with computer and information security training? These are the types of questions organizations should expect to see.

Underwriters will also scrutinize an organization's incident response and disaster recovery plans. They will review the organization's backup and recovery plans. There is a trend for underwriters to require Multi-Factor Authentication ("MFA") on all protected accounts and all outward/externally facing devices. Requirements for Endpoint Detection and Response ("EDR") also are becoming more commonplace.

Regardless of the new underwriting practices, resource-strapped CAHs should prepare to see a rise in attacks as larger systems deploy more sophisticated counter-measures, leaving the bad guys to target potentially more vulnerable sites. A successful ransomware attack can materially burden operations and increase costs if an organization's systems are offline for more than a short amount of time, as they often are. Hospital leadership also will be presented with the difficult choice of whether to make a ransom payment, which will depend on a variety of factors, including the nature of the data involved and whether reliable backups exist.

IBM released a report earlier in 2021 describing the Cost of a Data Breach. They showed that the health care sector has seen an average total cost of $9.23 million, the highest cost of all sectors in the report for 11 years in a row. Are CAHs prepared to absorb the cost of breach on top of the potential impact to operations resulting from a systems outage?

Is a "do nothing and hope for the best" strategy a viable approach for CAHs and cyber-attack preparation? The Ponemon Institute reported in September 2021 that nearly two-thirds of all patient care organizations have been victims of ransomware attacks. Business judgment and insurance underwriting requirements make clear that the time to act is now, and CAHs should not wait to prepare and equip themselves for this eminent threat. The preparations may also help offset impending cyber-insurance premium increases and other potential coverage limitations.

If you have any questions or would like more information on this topic, please contact:

- Mark Branstetter at mbranstetter@hallrenderas.com or at (615) 423-6651;
- Stephen Rose at srose@hallrender.com or (425) 278-9337; or
- Your primary Hall Render contact.

This article is educational in nature and is not intended as legal advice.