akerman

Blog Post

Healthcare Cyber Insurance? Fortify Your Defenses

July 6, 2022

By Kirk S. Davis and Danielle C. Gordet

Healthcare breaches, including ransomware attacks, continue to increase. As a result, many healthcare organizations seeking cyber coverage to help defray the costs associated with a ransomware attack or other data incident may find that carriers have increased premiums, reduced coverage, and tightened underwriting requirements. Healthcare organization leaders should understand that implementing reasonable administrative, technical, and physical safeguards to protect the organization's information and operational systems is not only required by laws such as HIPAA, but is increasingly required to obtain cyber coverage.

A recent report by Sophos, a technology security company, confirms this new reality. Sophos reported that one of the reasons for the growing demand for cyber insurance by healthcare organizations is the rampant growth in ransomware (Sophos Report). According to the Sophos Report, ransomware has led to more payouts and less profit for insurers, making cyber insurance coverage difficult and expensive to obtain, even driving some insurers out of the market.

The healthcare organizations surveyed by Sophos responded that:

- 66 percent experienced a ransomware attack in 2021;

Related People

Kirk S. Davis
Danielle C. Gordet

Related Work

Healthcare
Hospitals and Health Systems

Related Offices

Miami
Tampa

Health Law Rx

Akerman Perspectives on the Latest Developments in Healthcare Law

Visit this Akerman blog

- 78 percent have cyber insurance;
- 93 percent of respondents with cyber insurance had difficulty renewing the policies; and
- 45 percent of respondents with cyber insurance said the policies are incredibly complex.

Notwithstanding the complexity of the policies, the Sophos Report described the benefits of having that insurance in place. Indeed, 97 percent of insurers paid the damages for the most significant attack, 47 percent paid the ransom and many are paying huge cleanup costs to facilitate the healthcare organization's return to normal operation.

To qualify for cyber insurance in the current market, organizations must increasingly demonstrate that they have information security safeguards in place. For example, 97 percent of healthcare organizations responding to the Sophos survey noted that they changed their cyber defenses in order to have better cyber insurance positions. For example, they have increased staff training and education activities to improve cyber defenses, and/or implemented new technologies and services.

As summarized by the Sophos Report, other steps that can help healthcare organizations prepare for attacks and obtain cyber coverage include:

- Ensuring high-quality defenses are in place and periodically reviewing and updating security controls;
- Implementing tools to proactively hunt for threats in the organization's information systems and hiring Managed Detection and Response experts to provide out-sourced monitoring and response assistance;
- Reviewing the organization's environment to ensure that all security gaps are closed and utilizing an Extended Detection and Response platform to assist in collecting and monitoring threat data across the organization;

- Having an incident response plan in place and practicing it to be prepared should a cyber-attack occur; and
- Maintaining back-ups of the organization's critical data off-line and practicing restoring the back-ups to ensure minimal disruptions if an attack occurs.

Recent serious attacks demonstrate the urgency of this issue. Yuma Regional Medical Center in Arizona recently disclosed one of the largest ransomware attacks in the second quarter of this year (read more here). According to its notification to potential victims, individuals' Social Security numbers and other personal data were stolen. The facility's services remained mostly unaffected, however, thanks to backups and other emergency procedures. Yuma's experience demonstrates why healthcare organizations should invest in administrative, physical, and technical safeguards to protect their information systems. Doing so will better position such healthcare organizations in its efforts to obtain insurance coverage while minimizing the risk to the organization and helping them to meet their regulatory obligations.
