HEALTHCARE RISK MANAGEMENT™

THE TRUSTED SOURCE FOR LEGAL AND PATIENT SAFETY ADVICE FOR MORE THAN THREE DECADES

DECEMBER 2018 Vol. 40, No. 12

Expanding Cyberinsurance Market Brings Benefits to Healthcare

The expansion of the cyberinsurance market means that healthcare organizations can get more coverage for a lower premium than in the past, notes **Alex Purvis**, JD, partner with the Bradley Arant Boult Cummings law firm in Jackson, MS. Insurers also are building experience in paying claims, which helps them write policies that are realistic in terms of what they cover and what is excluded, he says.

Insurers focusing on cyberinsurance will have the best grasp and be able to pay legitimate claims, he says.

"The insurance policies that are cyberspecific tend to respond to the claims. The cyberinsurance industry tends to be a little more claim-friendly than you might see in some other insurance arenas," Purvis says. "That's another advantage to the market being so competitive now. These insurers don't want to get the reputation that they accept your premium dollars, but when you submit a claim they refuse to pay it based on some tiny language on page 12 of their insurance policy."

Some commercial general liability (CGL) insurance policies will cover the losses associated with a data breach, but that is becoming less common now that insurers recognize the size of that risk and prefer covering it with specific cyberinsurance policies, Purvis says. More CGL policies now specifically exclude the cyberrisk, making it more important to purchase a cyberpolicy, he says.

Purvis also cautions risk managers about the importance of putting the insurer on notice once a data breach or other covered cyberincident is discovered.

"What keeps me up at night as a policyholder lawyer is the fear that I've got a bunch of clients who are facing a claim but have not put their carriers on notice," Purvis says. "They may have a great insurance product, but if they don't put them on notice they may lose the opportunity get the coverage they've already paid for."

Consult IT Team

Healthcare organizations are adopting cyberinsurance more readily than in the past, says **Benjamin P. Malerba**, JD, partner with the Rivkin Radler law firm in Uniondale, NY. Policy limits for a hospital or other healthcare organization typically are between $3 million and $10 million, he says.

"You want to be sure that the coverage is not only going to provide you with defense against the cyberattack, but that it also will cover your costs related to a data breach, the notifications of not just the patients affected but also the government. In many cases, you will have to notify different branches of the federal government, law enforcement, and — since so much healthcare is delivered across state lines — multiple state governments," Malerba says.

Financial Disclosure: Author **Greg Freeman**, Editor **Jill Drachenberg**, Editor **Jesse Saffron**, Editorial Group Manager **Terrey L. Hatcher** and Nurse Planner **Maureen Archambault** report no consultant, stockholder, speaker's bureau, research, or other financial relationships with companies having ties to this field of study. Consulting Editor **Arnold Mackles**, MD, MBA, LHRM, discloses that he is an author and advisory board member for The Sullivan Group and that he is owner, stockholder, presenter, author, and consultant for Innovative Healthcare Compliance Group.

"Those costs can really add up. Even just the postage can add up if you have a large data breach, and there can be additional costs like writing the notification in several languages," he adds.

To obtain cyberinsurance, a healthcare organization's risk manager or compliance officer should first meet with an IT professional to determine the scope of the data and risk, and the security of the IT systems, says **Ananth Avva**, CFO at enterprise network security provider Lastline in Redwood City, CA. Consider factors such as whether you operate only in the United States, or internationally.

"Cyberinsurance insurers are also very good at customizing a policy to the needs of your institution. They can slice and dice the different options to tailor it for your needs, giving you a package that is commensurate with your level of risk," Avva says. "But for that to happen, you first have to have a good understanding of where your particular organization stands on these different factors that comprise your cyberrisk profile."

The most common error Avva sees when procuring cyberinsurance is having the CFO or compliance office drive the conversation with the insurer, when that person is not the one most familiar with the organization's data and risks. The IT department should be heavily involved in the purchasing effort, if not driving it, Avva says.

"If those two groups don't communicate and the CFO buys cyberinsurance just to check off a box somewhere, that's where you're going to see pretty big gaps," Avva says. "Cyberinsurance is not all the same, and you may discover later that the CFO or compliance officer didn't really understand what was covered and what was not. They don't understand it the same way the IT team does."

It is useful to think of cyberinsurance as filling in gaps in existing insurance coverage, says **Andrew Gibbs**, partner at the law firm of Lindabury, McCormick, Estabrook & Cooper in Westfield, NJ. While filling those gaps, a healthcare organization should strive to have overlapping coverage.

For example, an existing policy may already cover social engineering, the type of attack that uses psychological manipulation to trick users into making security mistakes or giving away sensitive information.

"Cyberinsurance can fill in gaps, and in some cases give you interlocking or overlapping coverage," Gibbs explains. "A large organization might have a crime policy with a social engineering endorsement, and then if you get a standalone cyberpolicy that also has social engineering coverage, you'll have an overlap. That overlap helps protect you because those policies are going to limits and exclusions that might be overcome by the other policy."

Cyberinsurance tends not to be expensive compared to other coverage, Gibbs says, but be careful to understand exactly what the policy provides. Deductibles should be considered carefully.

"There may be higher deductibles for certain kinds of cyberlosses, so healthcare organizations should get with their brokers or lawyers and try to maximize the coverage they can get within their financial restraints," Gibbs says. "They also should watch carefully for exclusions and language that lessens the coverage." ■

SOURCES

- **Ananth Avva**, CFO, Lastline, Redwood City, CA. Phone: (877) 671-3239. Email: aavva@lastline.com.
- **Andrew Gibbs**, Partner, Lindabury, McCormick, Estabrook & Cooper, Westfield, NJ. Phone: (908) 233-6800. Email: agibbs@lindabury.com.
- **Alex Purvis**, JD, Partner, Bradley Arant Boult Cummings, Jackson, MS. Phone: (601) 592-9923. Email: apurvis@bradley.com.
- **Benjamin P. Malerba**, JD, Partner, Rivkin Radler, Uniondale, NY. Phone: (516) 357-3128. Email: benjamin.malerba@rivkin.com.