Accessing the Benefits of Non-traditional Coverages through Captives: Cyber Liability Insurance

By Rocco Mancini and Kayla Salerno

The healthcare industry is the second-greatest utilizer of the captive insurance vehicle (Figure 1). Traditionally, healthcare organizations establish captive insurers to self-insure general liability, medical professional liability (MPL), other professional liability, and excess liability coverages. As the market for healthcare captives grows, healthcare organizations are showing an increasing interest in non-traditional lines of coverage: one of these is cyber risk.

More widespread adoption of electronic medical record (EMR) systems exposes healthcare organizations to unique cyber risks, such as those inherent in working with private health information (PHI), which is protected under the Health Insurance Portability and Accountability Act (HIPAA).

Background: captives in the healthcare industry
When compared with other industries that use captive programs, the healthcare industry has some unique, non-traditional risks and exposures. Many of these risks and exposures are substantial, and they can be difficult to insure. A lack of affordable coverage, sufficient coverage, or limits on the capacity of coverage in the commercial market for these risks is a potential issue for healthcare organizations. A risk that is relatively unique to the healthcare industry is MPL coverage.

MPL was the most common coverage written by healthcare captives in 2015, and in some cases, captives are formed for the sole purpose of providing coverage for this unique healthcare risk. In 2015, 14% of Marsh managed captives wrote standalone MPL coverage (Figure 2).

A captive may serve to expand an organization’s access to the commercial reinsurance market. In 2015, 33% of Marsh-managed healthcare captives accessed MPL reinsurance.

As the number of large health systems continues to increase, new exposures begin to emerge. Of these emerging exposures, cyber risk may be the most unknown (and difficult to assess) exposure, but it is also one of the most significant.
Any entity that transacts business over a computer network is exposed to cyber risks. Healthcare organizations are no exception. The advent of electronic medical record (EMR) systems increased exposures to cyber risk in the healthcare industry, and it also created cyber risk exposures that are unique to the industry. Most, if not all, healthcare organizations will handle protected health information (PHI) that is protected under HIPAA. As this information transitions from paper records to electronic records, it creates substantial cyber risk exposures. For this reason, it’s important for healthcare organizations to recognize the different types of cyber risk.

One commonly overlooked cyber risk is internal error. Concentra Health Services (Concentra) filed a breach report with the U.S. Department of Health and Human Services’ Office for Civil Rights (OCR), after an unencrypted laptop was stolen from one of its facilities. The OCR investigation revealed that Concentra previously had recognized the risk of leaving its electronic devices that contained PHI unencrypted. Concentra had begun to implement encryption on the devices containing PHI, but they were unable to fully implement the encryption before this event occurred. Ultimately, Concentra agreed to pay $1,725,220 in settlements for the potential violations caused by the exposure of the PHI. This settlement does not include the costs required to rectify damages as a result of any other private information that might have been lost, such as names, addresses, and Social Security numbers. The costs of these damages, or the costs needed to rectify the error, are often substantially greater than the HIPAA settlements.

The Concentra cyber breach raises an important but often overlooked point to consider when assessing an organization’s cyber risk exposures. Internal errors are a source of cyber risk that is often preventable, but it is also as unpredictable as cyber attacks. Although an organization may not be a common target for a cyber attack, it can still become the victim of a costly cyber breach.

Cyber risk is a new, emerging, and unknown risk. It is becoming increasingly difficult to access appropriate coverage for cyber in the commercial market; it may not be affordable. Amidst growing concerns of cyber attacks in the wake of several high-profile cyber breaches in 2015, commercial market premiums for cyber coverage increased substantially.

As it becomes more difficult to access cyber risk coverage in the commercial market, it also becomes much more difficult to find suitable limits and coverage for an organization. Cyber risk exposures can differ significantly between two organizations. Healthcare organizations also have another exposure, in PHI, which adds an additional variable.

Healthcare captives can be the ideal vehicle for accessing cyber risk coverage. Increasing premiums and diminished access on the commercial market means that a healthcare captive can provide an affordable alternative for cyber risk coverage. Also, a healthcare captive can be set up so as to offer cyber risk coverage that is specifically tailored to the needs of the insureds. It can offer limits that are difficult to access or prohibitively costly on the commercial market.

Most important, it can offer healthcare organizations more control over their cyber risk programs. This additional level of control is invaluable. Combined with strong risk management and cyber risk pro-

| Figure 2. Top Five Healthcare Captive Coverages (Reinsured Percentage Is Shown in Parentheses) |
| Professional Liability | 22% (20%) |
| General / Public / 3rd Party Liability | 22% (23%) |
| Medical Malpractice Liability | 14% (38%) |
| Excess Liability | 6% (88%) |
| Workers’ Comp / Employer’s Liability | 6% (18%) |

Captive Liability | 22% (20%) |
General / Public / 3rd Party Liability | 22% (23%) |
Medical Malpractice Liability | 14% (38%) |
Excess Liability | 6% (88%) |
Workers’ Comp / Employer’s Liability | 6% (18%) |
grams, it can give a healthcare organization the tools that it needs to secure and protect PHI from cyber breaches. Finally, the captive can be used to meet the organization’s cyber risk coverage needs by providing greater access to the reinsurance market. Taking these benefits into consideration, the healthcare captive has the potential to become a strong alternative market, if not the market, for cyber risk coverages.

New Exposures Continue to Emerge
Cyber risk is only one of the exposures that will continue to increase as consolidations and mergers create larger health systems. Another important risk to consider is terrorism risk. As health systems grow larger, the risk of terrorism risk is increased correspondingly. Captive insurers have the ability to access affordable coverage through the Terrorism Risk Insurance Act (TRIA), and that will be the subject of a discussion in a subsequent article.

References
1. Marsh 2015 Captive Benchmarking Report

Rocco Mancini and Kayla Salerno are Captive Advisory Consultants with Marsh Captive Solutions.