PARKER | SMITH | FEEK

COMMERCIAL INSURANCE
EMPLOYEE BENEFITS
PERSONAL INSURANCE
RISK MANAGEMENT
SURETY

PRACTICE GROUP:
HEALTHCARE

JUNE 26, 2018

HEALTHCARE CYBER 2.0 – UNDERSTANDING UNDERWRITERS' ANALYSIS AND PRICING OF YOUR CYBER EXPOSURES

Jim Chesemore | Principal, Chief Operating Officer

OVERVIEW

Much has been written over the past five years about the necessity of healthcare finance officers and risk managers understanding the different available risk transfer options to mitigate exposure to losses suffered from a cyber event. The loss of sensitive third-party health information is a significant threat to the reputation of all healthcare facilities. This paper moves beyond a basic overview and understanding of the myriad insurance products and services available to healthcare facilities today. The purpose of this paper is to give hospital risk managers or healthcare professionals an understanding of how the underwriting and pricing of these risk transfer (insurance) products has evolved and will continue to change. As breaches of sensitive third-party health information have occurred over the past five years, underwriters have a greater understanding of how to analyze their risk exposure and price their products to allow for greater long-term profitability of this segment of their insurance portfolio.

BEYOND INDUSTRY SEGMENTATION

An article titled, "Health Industry Lacks Patient Data Safeguards: poll"[1] highlighted that new technologies

> [T]he healthcare industry has higher cyber claims frequency because of the rigorous information security and privacy standards of the Health Insurance Portability and Accountability Act (HIPAA).

continue to flood the healthcare industry, yet the industry has struggled to prepare appropriate safeguards to protect their patients' sensitive health information. There is a massive push by healthcare facilities to adopt and incorporate the latest and best technologies to achieve greater efficiencies, while also ensuring their organizations are seen as cutting edge. This push has the unintended consequence of leaving healthcare facilities with the burden of ensuring they are building the right security to protect their systems and data. Identity thieves are using new methods to steal information, and targeting new types of accounts and services. Nowadays, these criminals go far beyond attacking just the familiar credit, debit, checking, or savings accounts. Phone services, cable and satellite television services, utility and electricity accounts, internet payment services, medical insurance, mortgages and rental housing, automobile and boat financing and

continued >

loans, and even government benefits are all susceptible to these kinds of attacks. Even more problematic, thieves will sometimes use stolen identities to avoid arrest when confronted by police or to obtain employment.

> The defining characteristics of cyber insurance risk exposures are interdependent security, correlated failure, and information asymmetry.

When underwriters first began to analyze and price cyber insurance policies, their focus was simply on industry segmentation and revenue size. Different industries are held to different standards. For example, the healthcare industry has higher cyber claims frequency because of the rigorous information security and privacy standards of the Health Insurance Portability and Accountability Act (HIPAA). Insurers only assessed insureds based on their location and industry. They then used their best judgment to identify which companies were most likely to be attacked. Intuitively, underwriters knew that healthcare facilities posed one of the greatest risks for cyber claims due to the vast amounts of third-party healthcare and private information that are stored on their I.T. networks. As was suspected, healthcare facilities have generated, outside of retail, the greatest frequency and severity of claims to date for insurance companies. When claims began coming through to the various insurance carriers, the insurance industry responded by developing greater underwriting capabilities that have required new and expanding expertise to improve risk selection and pricing. Those insurance companies writing coverage for healthcare facilities are now effectively segmenting their capacity to those facilities that meet or exceed their underwriting benchmarks. As innovation and digitization evolves, insurers have implemented the following key analyses to their evaluation and pricing of individual healthcare facilities.

RISK MODELING

According to the Canadian Institute of Actuaries, "Many organizations are 'living below the security poverty line.' Cybersecurity budgets for many midsize and small companies are minimal. As a result, those companies often have little or no I.T. expertise, are unable to follow through on I.T. consultant recommendations and accordingly focus only on 'putting out fires' rather than managing long-term cyber risk issues."[2] I.T. security vulnerabilities have shown almost no signs of improvement over time for most healthcare facilities. Underwriters are charged, therefore, to determine what risks have adequately adopted industry leading security programs and policies in their screening, evaluation, and pricing of potential cyber liability clients.

The defining characteristics of cyber insurance risk exposures are interdependent security, correlated failure, and information asymmetry. Some of these properties are common to all insurance markets, while others are unique to the risks of networked computing systems and cyber insurance for healthcare facilities. First, interdependent security reflects the degree to which the security of one computer network is affected by another system's compromise. For example, the security of a hospital's main systems may be compromised if an employed provider's home computer or PDA is allowed full access. Second, correlated failure (also known as systemic risk), is the systematic failure of multiple, disparate systems due to a single event. Correlated failures may occur in multiple ways, such as from a single source (e.g. a criminal group attacking many healthcare facilities), failure of a single I.T. system

continued >

upon which many businesses operate (e.g. cloud provider or virtualization data center), or compromise of many devices due to a common vulnerability or exploit (e.g. a distributed denial of service attack). Finally, information asymmetry in the context of insurance reflects the familiar moral hazard and adverse selection problems arising most notably from unsophisticated employees.

It should be emphasized that, while there are ways of reducing information asymmetries, most insurance

carriers are concerned with correlated failures because it defines the degree to which a security breach by one firm affects another. Most healthcare facilities are focused upon and concerned with interconnected nodes because this determines how a failure by a business partner may affect them.

Frequency and severity of events is the holy grail of cybersecurity risk management. While companies can analyze the frequency of cyber incidents based on some available data, estimating the severity proves more problematic. So how has the underwriting and pricing evaluation process evolved? Here is a brief overview of the changes.

1) Although revenue is one factor in the risk modeling evaluation, today's more important question is, how many patient records are housed in your facilities system? Underwriters want to understand the potential severity of a large breach on your system. You will be asked this question in the underwriting process.
2) Most underwriters have access to, or are themselves, former I.T. risk security professionals. Underwriters are scoring each risk based upon the answers to their applications' I.T. security questions. I.T. professionals now analyze the security's level of sophistication and the degree to which the individual healthcare facility's systems compare to benchmark I.T. security protocols. People who understand I.T. security are the ones who judge the quality of the risk.
3) The three most important questions that underwriters focus on in the application process are HIPAA compliance, encryption at rest, and PCI compliance.
4) Underwriters will utilize other information not asked for on applications in order to evaluate and price. These include:
    a. Whether the facility has a compliance and I.T. security agenda with timeframes that they are willing to share with prospective underwriters
    b. Copies of the most recent PEN Testing results
    c. Whether the facility has a written guide or set of protocols that address the protection of customer assets (information) that they are willing to share with underwriters
    d. Copy of the facility's breach response plans

APPLICATION PROCESS

The application questionnaires provide insights into the security technologies and management practices that are examined by carriers. For example, most insurance

continued >

companies today include four main specializations: organizational, technical, policies and procedures, and legal and compliance. Healthcare professionals have witnessed the growing length of cyber applications. Underwriters continue to expand their questions and data gathering to appropriately select and price risk and ensure they meet their target ROI for healthcare insurance. Underwriters are expanding their questions of third-party service and supply chain providers.

The United States' cyber insurance market has been growing rapidly over the past decade. With less than one billion dollars in premium in 2012, most experts estimate that this market will grow to $20 billion by 2020.

While the cyber insurance market has reached a significant size since its inception, it remains a small component of the overall insurance market. As of 2015, the year in which the cyber insurance market reached $2 billion, the net premiums in the commercial insurance market totaled $247 billion. However, not unlike earthquake and flood coverage, cyber risks have the potential to generate huge losses for the insurance industry. Underwriting selection and pricing will continue to grow in sophistication, and healthcare professionals need to spend the time on these applications and supporting materials to assist their insurance broker partner give a positive and accurate image of the facility's ability to fend off and respond to cyber breaches.

1. https://www.reuters.com/article/us-privacy-poll/health-industry-lacks-patient-data-safeguards-poll-idUSTRE78L0ZD20110922
2. https://www.soa.org/sections/joint-risk-mgmt/cyber-security-impact.pdf