RISK CONSULTING PERIODICAL

HEALTHCARE RISK EDITION

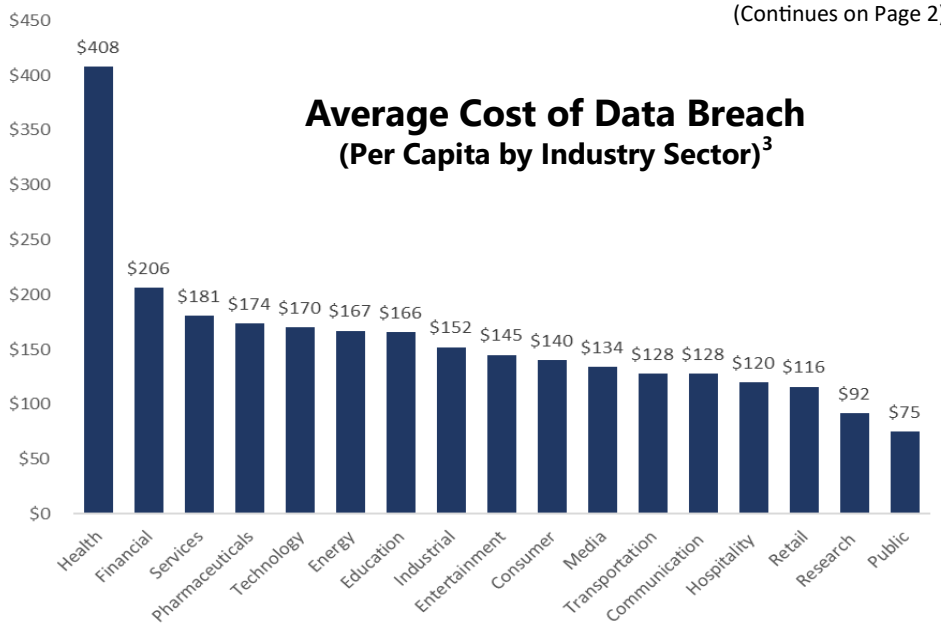
Quarter 1, 2020 Volume I

In the US, stolen personal health information can be used by criminals to obtain expensive medical services, devices and prescription medications, as well as to fraudulently acquire government benefits like Medicare or Medicaid.

For the first six months of 2019, breached patient records doubled the total for 2018 from 14,2M to 31.6M affected patient records in 285 disclosed incidents reported to the U.S. Department of Health and Human Services (HHS).[1] The material uptick in breached patient records during the first half of 2019 is attributed to the American Medical Collection Agency (AMCA) breach affecting over 20M patient records.[2] Absent this outlier breach, 2019 is on track to exceed 20M patient records breached, or a 40% annual increase in 2019 v. 2018, based on current trends.

Data breaches cost the healthcare sector an average of $6.5 million per breach, over 60 percent more than all other sectors, according to a Ponemon Institute report, sponsored by IBM. Other sectors spend about $3.9 million, on average. Ponemon researchers interviewed 500 global organizations that experienced a data breach in the last year. The researchers found for the ninth consecutive year the healthcare sector is still the hardest hit financially by data breaches.[3] The Ponemon report also found breach costs have increased 5 percent in healthcare in the past year. In fact, health providers will spend $429 per each lost or stolen record – up from $408 per record in 2018. The cost is about three times more per record than all other sectors. At $429 per patient record breached. Assuming that the average cost is $6.5M per breach at $429 per patient record, the reverse-math indicates that the average number of patient record breached is approximately 15,000 patient records breached per incident. This compares with

(Continues on Page 2)



CYBER LIABILITY INSURANCE: UNDERSTANDING THE VARIOUS INSURING AGREEMENTS

The use of the term "cyber insurance policy" is somewhat of a misnomer, as few carriers or policy wordings refer to that term. Instead, today's best-in-breed coverage is referred to as an "Information/ Network Security, Privacy, Multi-Media and Data Breach Protection" policy. A few insurers in the U.S. and London markets are now even offering menu driven products that can be tailored to only include the insuring agreements that your firm needs, avoiding unnecessary expense for insurance agreements that your firm has little or no insurable risk. Typically, there are about a half-dozen insuring agreements available in a standard off-the-shelf "cyber" policy. In order to better understand the various coverages available and how they may or may not be beneficial from both a protection and cost-benefit standpoint for your particular financial services firm or fund, the following primer is intended to provide transparency on this otherwise opaque product.

(Continued on page 2)

RISK CONSULTING PERIODICAL

Quarterly review of medical malpractice, professional and management liability trends, coverage issues, complex claims coverage and related litigation trends impacting healthcare delivery.

2019 may prove to be the worst seen for healthcare cybersecurity. It is estimated that security breaches will cost healthcare organizations $6 Trillion Dollars by 2020

(Continued from Page 1)

the top 5 provider breaches in the first six months of 2019 as follows:

1. University of Washington Medicine: 973,024 patient records breached;
2. Oregon Department of Human Services: 645,000 records breached;
3. Columbia Surgical Specialist of Spokane: 400,000 records breached;
4. UConn Health: 326,629 patient records breached; and
5. Navicent Health (Georgia) : 278,016 patient records breached.

Putting aside the outlier large breaches listed above, cyber liability insurance underwriters now possess increasingly reliable actuarial data for loss forecasting and economic damage assumptions.

The challenge that underwriters have is that not all breach exposures are created equal, and as such, how to adequately rate and assign an adequate premium to a specific healthcare risk. For example, the 2019 Mid-Year Data Breach Monitor report[1] shows that the first six months of 2019 was dominated by hacking incidents, which accounted for 60% of all incidents and 88% of breached (Personal Healthcare Information, or PHI) records. 21% of all breaches were insider breaches (rogue healthcare employee, other). Compounding the underwriting challenge factoring what the ultimate legal and economic losses that any particular healthcare provider risk may have and charging an appropriate premium.

Whereas underwriters can determine the approximate aggregate expense of breach notification cost of any particular healthcare risk (item # 4 in right column), estimating private litigation damages and governmental fines and penalties is considerably more difficult for underwriters. For example, the Department of Health and Human Services reported record fines of $28.7 million for breaches occurring in 2018. This included a record high fine of $16M for Anthem, Inc., the largest HIPAA fine ever issued, as the breach violated the electronic protected health information (ePHI) of some 79 million insureds. In addition to HHS fines and penalties, health-care providers are also subject to fines and penalties brought by state attorney generals. And finally, defense cost, breach coach and remediation expenses (some carriers cover, other's not) and potential cyber extortion payments (see item # 6 to right are also difficult to predict. To learn more, contact RCP to learn more about our custom tailored insurance and risk solutions.

1. Protenus, Inc. 2019 Mid-Year Data Breach Monitor
2. Bankinfosecurity.com, June 19, 2019
3. Ponemon Institute, Cost of Data Breach Report, July 23, 2019
4. Health IT Security (www.healthitsecurity.com) July 23, 2019

CYBER LIABILITY INSURANCE

(Continued from page 1)

1. **Privacy, Information and Network Security Liability:** 3rd-Party claims (including defense expense) made against your firm that arise from a failure to protect clients and other third-parties' sensitive, protected and/or personally identifiable information from a hacker, rogue employee or other unauthorized person or entity (that is in your firm's care, custody and control). Coverage can extend to regulatory actions and fines and penalties in certain instances;
2. **Electronic Multi-Media Liability:** 3rd-party claims (and defense expense) for negligent acts that arise from content on corporate websites, social media, alleged intellectual property infringement (no patent or trade secret coverage), breach of license, defamation, invasion of privacy, other;
3. **Technology Errors and Omissions:** for claims against your technology-based firm from failure to perform your business activities for a client to a required standard as defined by a master service agreement (no market risk);
4. **Breach Notification Expense:** 1st-party reimbursement for breach notification services required by statute to notify affected individuals whose Personal Healthcare Information (PHI) was breached;
5. **E-Business Interruption:** 1st party reimbursement for net income loss; and;
6. **Cyber Extortion:** 1st party claims for the payment of ransom to a hacker threatening to damage your IT system, website, etc.

With over 20 years of public company D&O & Fund underwriting and brokerage experience, Scott has counseled clients of all sizes and complexity, from S&P 500 corporations to start -ups. Scott is a frequent speaker on executive liability topics.

SCOTT UHL • 214.238.7354 • suhl@rcpholdings.com

With over 30 years of medical malpractice and professional liability/general liability claims administration and brokerage experience, Mike has counseled hospitals, physician groups, managed care & skilled nursing organizations of all sizes and complexity.

MIKE JACOBY • 214.238.7358 • mjacoby@rcpholdings.com