Arthur J. Gallagher & Co.

# Market Conditions

JANUARY 2016


## Cyber Risk Insurance

Rapidly growing market at a crossroads

**By Adam Cottini**

### 2015 IN REVIEW

The year 2015 should be remembered as the year that the cyber insurance market took a first step toward risk engineering following the mega breaches of 2013 and 2014. With several insurance carriers demanding more information to better understand cyber risk, the pendulum swung back to additional underwriting data collection and more detailed conference calls with Chief Information Officers and Chief Security Officers.

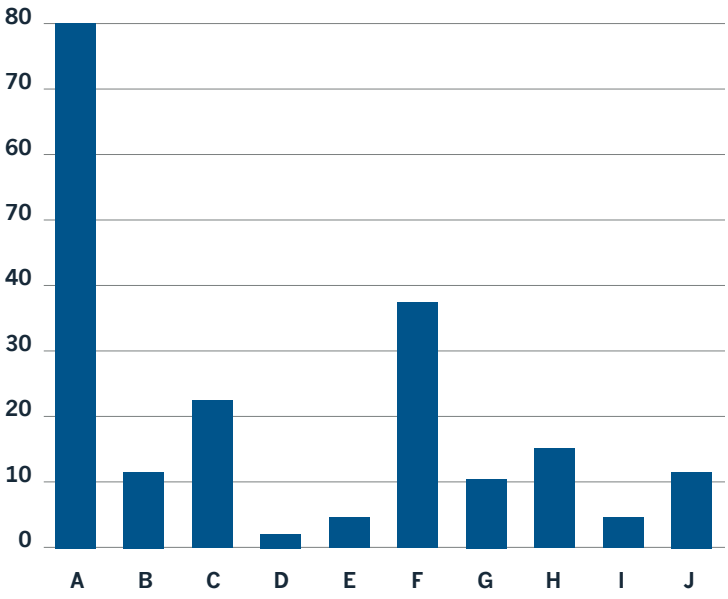
In addition, markets were in flux, with several carriers deciding to re-price or reduce participation in certain high-risk market segments, such as retail and healthcare and large risk business in general. These segments were impacted by the following scenarios:

- Primary underwriters significantly increased premium costs and retentions.
- To establish a more sustainable pricing level, rate hikes on excess towers began to outpace those of the primary underwriter, in many cases creating "hour-glass" pricing structures. Excess underwriters had recognized that they were charging insufficient premiums in those areas for the losses they were experiencing. The days of a $5,000 rate per million of coverage, which used to be the norm on excess placements, was no longer sustainable.
- Capacity was cut as excess markets sought to reign in the exposure that they had been accepting without sufficient premium to support their limits. This was prevalent among both primary and excess underwriters.
- In addition, some carriers drastically changed their risk appetite, ultimately deciding to cease participation at lower layers in excess towers, or to completely exit the cyber insurance business. In either scenario, the result was very disruptive to insureds. Holes created in many insurance program structures needed to be filled in a time of reduced capacity. This was particularly challenging for large towers of insurance.

**Demand for cyber insurance hit an all-time high**

Anthem's massive data breach started the year with a bang, triggering heightened awareness in the boardroom. Litigation previously unheard of in this line of business generated headlines as very large cyber insurance towers absorbed $50M–$100M each, in losses in breach mitigation and class action litigation defense related expenses.

**Top 10 Data Breaches of 2015**




● Individuals/Accounts Affected (Millions)

A Anthem, Inc.—1/29/15
B Premera BlueCross BlueShield—1/29/15
C Office of Personnel Management—4/15
D CareFirst BlueCross BlueShield—5/15
E UCLA Health Systems—5/5/15
F Ashley Madison—7/15/15
G Excellus BlueCross BlueShield—8/5/15
H Experian—9/15/15
I Scottrade—9/15
J Vtech—11/26/15

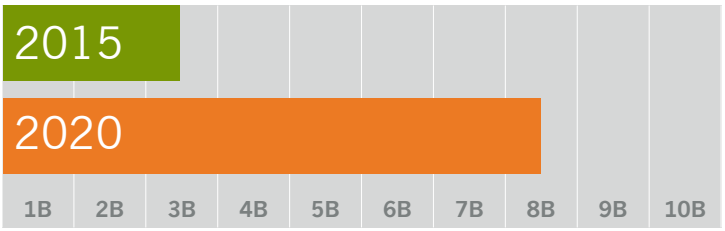
Arthur J. Gallagher & Co.

# Market Conditions


Not surprisingly, concern over cyber risk and those well-publicized financial losses has resulted in an increased demand for cyber insurance, as well as much more detailed underwriting from insurance carriers for certain classes and sizes of business.

The cyber insurance market, however, is still in growth mode. Not all classes of business are considered difficult to underwrite. Small to middle-market organizations in all industries, including retail and healthcare, are looking to obtain cyber insurance for the first time or to increase their coverage limits at renewal. Simultaneously, insurance carriers would like to balance their larger and riskier books of business with more diverse and less risky pools of insureds. The view forward suggests cyber insurance is very much a growth business in all categories of risk.

PwC's study on cyber insurance spotlights a worldwide market representing $2.5B in premium (90% of which is purchased by U.S. companies) at the start of 2015. Premiums are expected to grow to $7.5B by the year 2020. Today many insurance carriers and brokers are experiencing growth in cyber insurance business of 20% to 60% year-over-year.




- $2.5 billion in gross written premium (GWP)
- $7.5 billion in gross written premium (GWP)

## THE OUTLOOK FOR 2016

Insurance companies writing cyber insurance are competing for small to middle-market risks, defined as businesses with annual revenues of less than $500M. For organizations with revenues above $500M, there is increased scrutiny of those deemed as high risk due to heavy exposure of personally identifiable information (PII). Entities that may fall into this category are retail, healthcare, financial institutions, government and higher education. Those organizations that generate more than $1B in annual revenues are often deemed riskier regardless of their category. And sizeable entities within a high-risk industry can encounter significant difficulties in obtaining adequate capacity and reasonable pricing.

**Premiums & Retentions**

In 2016, it will not be uncommon to see major premium adjustments based on multiple factors, with the industry type and its exposure to breaches of confidential information driving these changes.

For the retail and healthcare verticals, rate increases of 15% to 40%+ are likely if revenues exceed $1B. In many cases, premium increases and elevated retentions should be anticipated. Within both sectors, don't be surprised to see declinations to offer future coverage and expect much larger rate increases in the excess layers of large towers.

All other industries will see less volatility, but we expect rate increases averaging 1% to 10% to be the norm, with retentions remaining at the same level. Competition for smaller and less risky cyber opportunities, for insureds with annual revenues of less than $25M, will likely create an environment where premiums actually decrease.

## PROGRAM STRUCTURE

Coverage will continue to be refined in the coming year. This comes as no surprise given the evolution of these products since their introduction 15+ years ago. Program structure will continue to be an issue, including such questions as:

- Where are sub-limits appropriate?
- Should a layered program or line slip/quota share be recommended?
- What is the appropriate mix between domestic and London capacity?

A larger concern that insurance carriers will need to affirmatively address is under which policies bodily injury and property damage from a cyber-attack will be covered.

Social engineering losses do not appear to be waning, providing a good example of the blurred lines between cyber and other coverage lines. Phishing attacks on accounting and finance personnel often result in erroneous funds transfers when employees comply with fraudulent requests or instructions from someone posing as a legitimate vendor, company executive, etc. Carriers have denied these claims under crime policies citing a number of exclusions, such as willful departure of assets, direct vs. indirect loss, etc. Similarly, cyber insurers have denied claims on the basis that there is no third-party alleging a privacy law violation, nor does it meet first-party loss insuring agreements. Recently, carriers have responded


by developing additional insuring agreements for "social engineering" losses, most typically under crime policies. Very few cyber policies have been written to address this exposure, although it seems a few insurers might be willing to do so.

In addition, there is a desire to expand business interruption to trigger coverage if a "dependent business" incurs security or system failure. All organizations will benefit from these expansions of coverage because the coverage may complement existing property policies affording similar coverage but not providing failure of security or system failure triggers. Industries that may consider this coverage extremely valuable include construction, energy and utilities, manufacturing, marine and transportation.

## THE ROAD AHEAD

Data breaches will continue to generate headlines and it is inevitable that several large breaches will be announced in the coming year. Litigation will play a role in loss development as more plaintiff-friendly jurisdictions start to set precedents. Underwriters will require more data from insureds than we have seen in prior years and proper cyber risk management protocols will be rewarded. As a result, we expect premiums and retentions in the coming year to range from small decreases to significant increases, depending largely on size, industry, operations and exposure to confidential information.

---

About the Author: Adam Cottini is the Managing Director in Arthur J. Gallagher & Co.'s Cyber Liability Practice and a member of Gallagher's Management Liability Practice. These practices focus on providing insurance and risk management solutions related to executive and management liabilities. For additional information, please contact Adam at Adam_Cottini@ajg.com or visit www.ajg.com/mlp.