BANKS SHOULD EXPECT SIGNIFICANT CHANGES TO UPCOMING CYBER LIABILITY RENEWAL

An increased dependency on virtualized services, especially over the past year, means that cyber liability ransomware claims have increased both in frequency and severity. Banks are more exposed than ever before to data risks, and these are problems that are not going away any time soon.

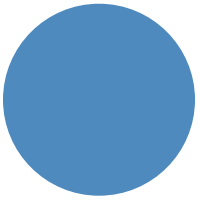
Mitigating cyber risk, especially around ransomware, has become a priority for IT and business leaders alike. These concerns are warranted, especially for financial institutions. The May 2021 Kroll Cyber Briefing reports that financial institutions remain in the top four industries impacted by ransomware attacks.

Additionally, according to the NetDiligence 2021 Ransomware Spotlight Report, in the past five years, the average ransom demand has shot up almost twelve-fold, from $15,000 to $175,000. In The State of Ransomware 2021, Sophos surveyed 5,400 IT decision makers across 30 countries and found that 37% of respondents were hit by a ransomware attack. Of those respondents, 54% said the cybercriminals succeeded in encrypting their data. After paying ransom, on average only 65% of encrypted data was restored to organizations. When accounting for system downtime, loss of revenue, cyber investigation costs, legal costs and any ransom paid, this report also estimates the average bill for rectifying a ransomware attack was $1.85 million. In this increasingly risky environment, financial institutions are turning to cyber insurance to protect their assets.

Traditional bank cyber liability policies offer a suite of broad coverages at a price point that is typically much less costly than the other management liability coverages. There is also another significant comparison between cyber and other coverages that is influencing the carrier responses. In the scenario of a D&O or E&O claim, the covered legal fees and ultimate settlement or judgement can accumulate over the period of years and several renewal cycles. The insurance carriers have a lot of time to determine the loss reserves for these claims and several renewals to make up the premium.

However, in the case of a covered ransomware claim, the damages, which are in the hundreds to thousands or even millions, are felt immediately. Carriers then associate these losses with a premium level that would require decades to recoup. With these claims increasing in both frequency and severity, cyber carriers are having to compensate for the losses in a quick and sometimes drastic fashion.

Interested in learning more about the state of cybersecurity? BRP's MiddleMarket firms hosted a webinar, "The Evolving Cybersecurity Landscape", which provides more detail and analysis about these topics. View a recording of the webinar here.



Dennis Gustafson
Partner, Financial Institutions Practice Leader - AHT
Dennis.Gustafson@ahtins.com

AHT INSURANCE
A BALDWIN RISK PARTNER

The cyber renewal period of 2021 impacted our banking clients in two distinct ways:

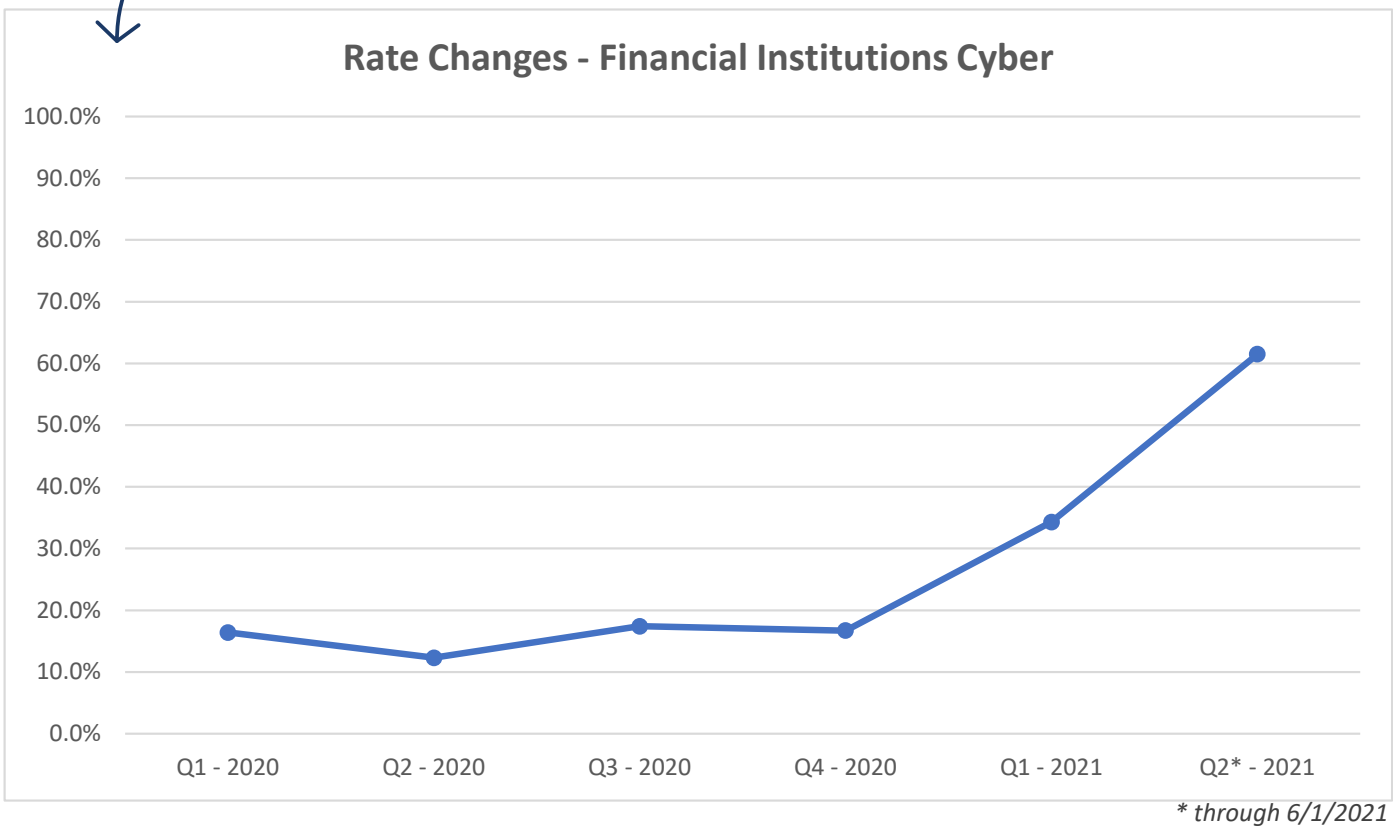
1. Request for a lot of additional information. Prior to 2021, we saw cyber applications with as little as four or five basic questions. Dedicated ransomware applications are now very common, and highly specific Mufti-Factor Authentication (MFA) questionnaires are the norm. See an accumulation of Ransomware/MFA questions we received from different underwriters. You should expect to have to answer at least a subset of these.

2. Cyber premiums are increasing. And, in instances where responses to the questions shared above have answers underwriters see as red flags, we are also seeing increased retention and restrictive coverages. Here is a snapshot of cyber rate increases for financial institution clients.

In a marketplace that is changing so quickly and dramatically, it is very difficult to predict what the next month could look like, much less the next year.

Optimistically, the hope is that as a community, we have learned enough about the different breach scenarios to implement strategies and technologies that will protect us from such attacks in the future. This will minimize the possibility of ransomware attacks occurring and stabilize the cyber marketplace.

On the other hand, we may continue to see a slew of these losses. It is not entirely unrealistic to imagine a scenario where ransomware and other cyber extortion attacks are completely removed from cyber liability policies either to be determined as uninsurable or offered on a stand-alone basis, as is the case with Kidnap & Ransom coverage.



** through 6/1/2021*