Gallagher

Insurance | Risk Management | Consulting

Market Conditions

FEBRUARY 2021

THE 2021 CYBER INSURANCE MARKET CONTINUES TO HARDEN

Author: John Farley, Managing Director, Cyber Practice

For the majority of its relatively short life, the cyber insurance market saw rapid expansion and nimbly evolved to meet changing cyberthreats. Cyber insurance buyers enjoyed expanding coverage terms, plentiful capacity and flat to falling rates in a highly competitive marketplace. However, as we reported last year, the cyber insurance market hit an inflection point in late 2019. Carriers became pressured due to the increasing frequency and severity of cyber claims and a more stringent regulatory environment at the state, federal and international levels. 2020 began with the first real signs of a hardening market as the larger, more sophisticated risks in specific industry sectors became subject to greater underwriting scrutiny and ultimately increased premiums. That trend continued and accelerated into the latter half of 2020, and we expect it to become even more challenging in 2021.

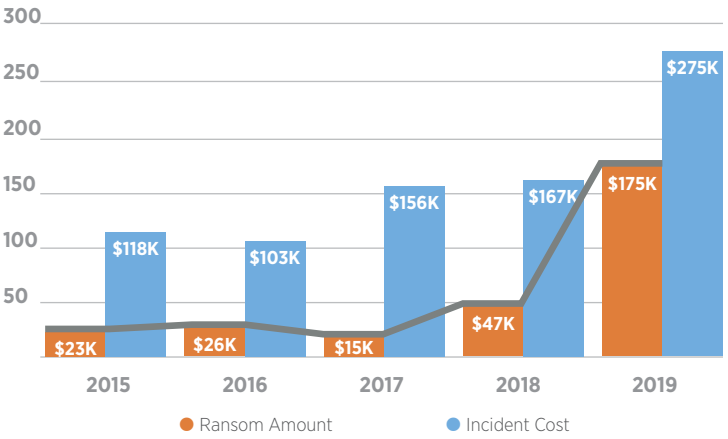
THE THREAT LANDSCAPE

Most cyber insurance professionals will agree that the hardening market is primarily being driven by ransomware attacks. We have seen a disturbing trend, as hackers became more calculating in who they targeted and the amount of ransom they expected to collect, and used sophisticated ransomware variants to execute their attacks. Today's ransomware attacks often target managed security service providers (MSSPs) that frequently act as the outsourced IT vendor to hundreds, if not thousands, of other companies. By attacking them, hackers can impact all of the MSSP's clients in one efficient cyber attack. Unlike ransomware attacks in previous years, today's cybercriminals have drastically increased their extortion demands by routinely demanding six-figure sums to release data, with occasional extortion attempts reaching multimillion-dollar amounts. Failure to meet these demands often results in threats to release the victim's most sensitive data to the public, as the newest ransomware variants work to not only freeze data, but to also exfiltrate data. This often creates legal liability for the victim company, including mandating notification to affected individuals and regulators, on top of what often results in significant downtime, unforeseen extra expenses and lost business. In fact, a recent study by Coveware revealed that the average downtime due to a ransomware attack is 19 days.[1] That extended downtime often leads to lost business costs that are exponentially greater than the extortion demand itself. What makes matters worse is that these attacks are disproportionately impacting small and medium-size enterprises that are often least able to defend and mitigate the attack. According to Coveware, 70% of ransomware attacks are aimed at organizations with less than 1,000 employees. While the lack of protection in the face of these attacks is a grave concern, it is heightened by the fact that the losses for these organizations are often uninsured, as only 10% of them purchase stand-alone cyber insurance policies, according to Gallagher Drive data.[2]

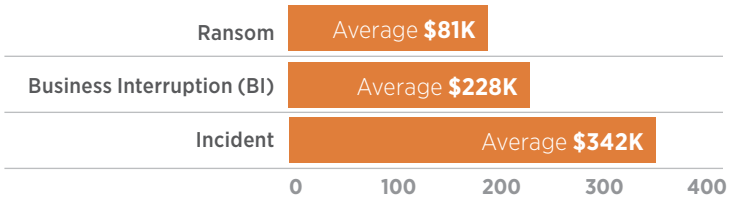
Focus on Ransomware

Leading Cause of Loss for SMEs

AVERAGE COSTS BY YEAR



RANSOMWARE THAT INCLUDED BUSINESS INTERRUPTION



Another leading cyber claim cost driver can be attributed to social engineering schemes that lead to funds transfer fraud. These most often manifest via business email compromise and invoice fraud. The FBI validated this trend when they released their Internet Crime Report in 2020, which indicated that victims sustained $1.7 billion in losses due to business email compromise in 2019.[3]

Market Conditions

FEBRUARY 2021

Several leading cyber insurance carriers documented these trends in their own studies.

- **Axis:** There was a 404% increase in ransomware demands from 2018 to 2019.[4]
- **Beazley:** Middle-market companies (over $35 million annual revenue) were increasingly targeted for social engineering and fraudulent instruction. These attacks Increased from 46% in Q1 2020 to 60% in Q2 2020.[5]
- **Coalition:** The most frequent types of losses were ransomware (41%), funds transfer loss (27%) and business email compromise incidents (19%).[6]

COVID-19 AND INCREASED CYBER RISK FOR REMOTE WORKERS

The sudden onset of COVID-19 forced many employers to pivot to remote working environments, with little time to secure them. Almost immediately, cyber intelligence sources revealed multiple phishing campaigns aimed at remote workers. Compounding these cybersecurity threats was the fact that many workers operated in an inherently risky ecosystem consisting of personally owned devices, public WiFi, web conferencing platforms and remote desktop protocol that may not have been securely configured. In fact, insurance carrier Coalition's 2020 claims study revealed that exploiting the remote workforce was the leading cause of ransomware claims during pandemic.[7] We expect the remote workforce to continue operating well into 2021 and beyond, making this an additional frontier for Chief Information Security Officers to secure.

NATION STATE THREATS AND SYSTEMIC CYBER RISK

In December, a far-reaching hacking campaign was revealed by top U.S. government officials that has been attributed to nation-state actors. Targets included the U.S. Departments of Defense, Homeland Security, State, Treasury, Energy and Commerce, as well as several others. The attack extended to the private sector and may impact several thousand organizations. Initial investigation indicated hackers were able to exploit flaws in a widely used software program that provided a back door for access to any company that performed routine updates of the software product. While we will not know the full extent of the attack for several months, the reaction of the cyber insurance market was swift. Within days of the attack, we saw at least one major cyber insurance carrier add exclusionary language specific to the use of this software product to be imposed upon policy renewal.

INCREASING REGULATORY RISK

Following the trend of recent years, regulators on a variety of levels continue to focus on privacy rights of individuals while flexing their regulatory powers by imposing new data collection and protection requirements, and ultimately levying fines and negotiating settlements for noncompliance. While most regulation has not had a direct material impact on cyber insurance rates to date, we do expect it to become a more significant factor as we see clear evidence of more aggressive enforcement trends.

- **International regulation:** In 2020, the EU-U.S. Privacy Shield, which allowed U.S. companies to transfer data from the EU to the U.S. through a self-certification process, was replaced with specific standard contractual clauses. We expect this will pose greater difficulty from both an operational and compliance perspective.

  In other developments out of the EU, we took note of significant enforcement of the General Data Protection Regulation (GDPR). In the first 10 months of 2020, there were 220 fines issued, amounting to payments of 175 million euros. There is clear evidence of an increasingly aggressive trend in GDPR enforcement since its passage in 2018. Comparing fines issued between the time periods of July 2018 through June 2019 and July 2019 through June 2020, there was a 260% increase in fine frequency.[8]
- **Federal regulation:** In 2020, we saw the second-largest HIPAA settlement ever, amounting to $6.8 million. The Department of Health and Human Services' Office of Civil Rights agreed to a settlement with a HIPAA-covered entity that they allege did not detect a data breach for nine months that impacted 10.4 million individuals.[9]

In late 2020, the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) issued an advisory stating that making ransom payments to cybercriminals that are subject to OFAC sanctions may violate OFAC regulations and result in civil penalties.[10] While these compliance requirements were in existence for several years, the advisory specifically clarified that they apply to companies involved in providing cyber insurance, digital forensics investigations, incident response firms and financial services companies that facilitate the processing of ransom payments. However, as of this writing, we have not received any indication that this will significantly change terms and conditions of cyber insurance coverage being offered by the overall cyber insurance market. It is also important to note that, to our knowledge, the majority of ransomware claims received by most cyber insurance carriers historically have not involved OFAC-sanctioned entities, regimes or persons.

Market Conditions

FEBRUARY 2021

- **State regulation:** Several states, including Illinois, Washington, Texas and Arkansas have either enacted or amended privacy laws related to the collection, use and retention of biometric data. There has been a significant uptick in litigation related to biometrics, including a recent $650 million settlement involving a class of Illinois residents.[11] We are closely watching the proposed National Biometric Information Privacy Act of 2020, which could significantly expand biometric regulatory requirements across the United States.

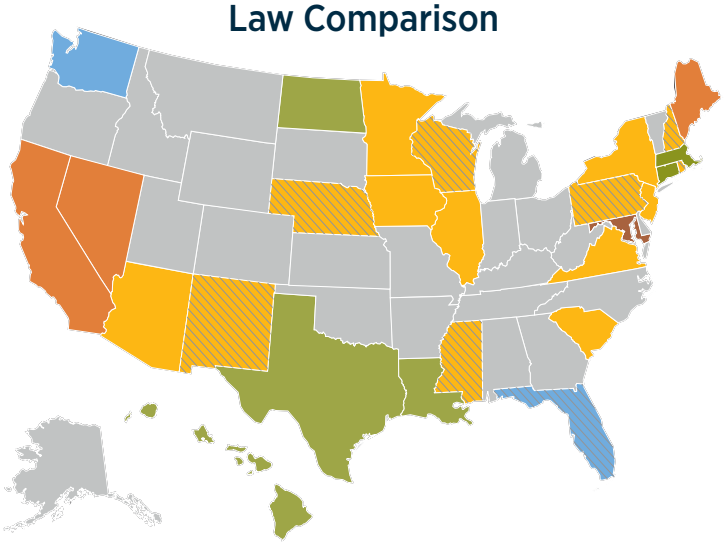
In addition, several states have followed the California Consumer Privacy Act, aimed at granting U.S. citizens greater control over their personal data. Many are requiring businesses to comply with these rights, as over half of all states have introduced legislation or passed laws to that end. Notably, many states are proposing private rights of action, which we expect will drive litigation costs.

CYBER INSURANCE COST DRIVERS ON THE RISE

The cyber insurance market has responded to increased cyber claim frequency and severity with pricing momentum that trended upwards throughout most of 2020. We expect the cyber underwriting community to continue to seek the highest increases from organizations with annual revenue in excess of $100 million and become ever more wary of any organization that falls within specific sectors, including municipalities, healthcare, financial services, higher education and technology. Ultimately, we are projecting rate increases in the range of 15% to 50% for cyber insurance buyers.

We also expect 2021 cyber underwriting practices to evolve from narrowly focusing on risk factors such as revenue, number of employees, record count and industry class. We will see a wider underwriting lens that will expand to an increasing use of loss modeling tools and continual system scanning, utilizing both in-house and outsourced IT security resources as they evaluate prospective insureds.

State-Comprehensive Privacy Law Comparison

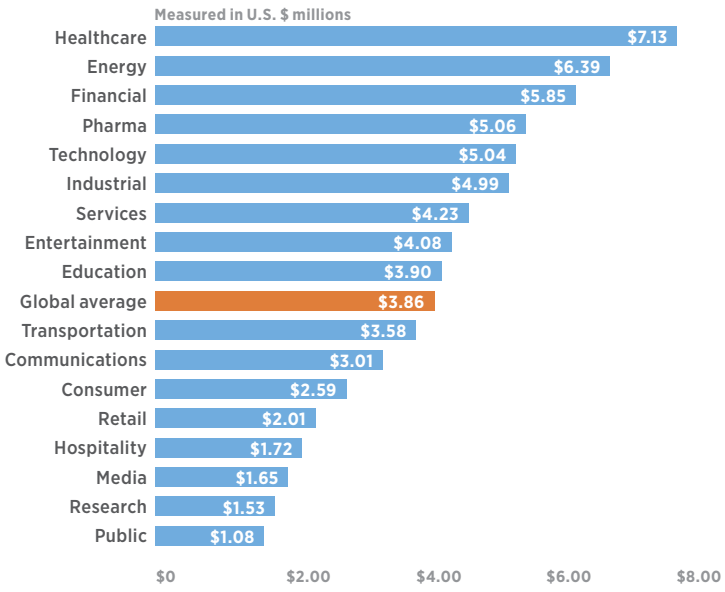


- Task force substituted for comprehensive bill
- Bill died in committee or postponed
- None

Statue/Bill in Legislative Process:

- Introduced
- Cross-chamber
- Passed
- In committee
- Cross-committee
- Signed

Average Total Cost of Data Breach by Industry



Market Conditions

FEBRUARY 2021

There is also a likely scenario that we see constricting of capacity in the market, which may drive pricing up further. There is evidence of primary markets looking to avoid specific industry sectors that they previously pursued. Even excess carriers are taking a cautious approach by offering lower limits than they may have in recent years. We expect cyber insurers to seek greater protection from the reinsurance market, which may in turn seek out protection for its own potential losses from the retrocession insurance market. These new cyber insurance structures will be in focus in 2021 as fears of aggregation risk, which is of particular concern and illustrated in cyber catastrophe scenario models, begin to mount. In addition, we have seen one major cyber insurance carrier impose sublimits and coinsurance specific to ransomware attacks. We expect others to follow as long as the 2021 ransomware claims trends follow the trajectory we saw throughout 2020

- Please note, a client's risk profile is the primary variable dictating renewal outcomes. Loss experience, industry, location and individual account nuances will also have a significant impact on these renewals

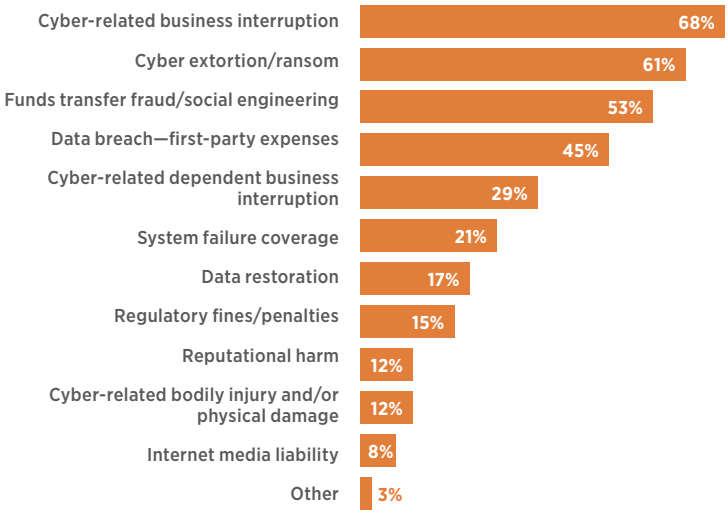
At the same time, we expect risk managers to sharpen their focus on cyber insurance products that can effectively transfer the risks associated with the latest cyber attack trends. This was documented in a 2020 survey by Advisen and PartnerRe,[12] where the top three coverages sought were cyber-related business interruption, cyber extortion/ransom and funds transfer fraud/social engineering, respectively.

STRATEGIES TO NAVIGATE THE HARDENING CYBER INSURANCE MARKET

Despite the concerning signs of a hardening market, we do see opportunities for the cyber insurance buyer to navigate the challenges that 2021 will bring. The market will look to incentivize those organizations that are willing to entertain higher self-insured retentions. Historically, the vast majority of our clients choose to self-insure under a $25,000 threshold.[13]

Q

What cyber coverages are (new and renewal) buyers most interested in purchasing? Please select top three:



Those that assume more of their own risk in the form of higher retentions will be compelled to embrace cyber risk management techniques in ways that they may not have before. They can do this by leveraging pre-breach vendor services that come free or discounted as part of the cyber policy's cyber risk prevention and mitigation services. Almost all cyber insurance carriers offer their clients some form of employee training, incident response planning, table top exercises, compliance assistance, technical IT security services and other valuable tools. Ultimately, greater use of these resources will shine a more positive light on most buyers as they enter the market.

As we look forward to 2021, it is clear that the cyber insurance marketplace has undergone a paradigm shift in the way cyber risk is underwritten and ultimately transferred. Cyber risk will continue to evolve and markets will react accordingly, and quickly, to modify terms, conditions and capacity. The buyer will need to be mindful of these dynamics as they navigate what promises to be a challenging year for everyone in the entire cyber risk management ecosystem.

Market Conditions

FEBRUARY 2021

John Farley, Managing Director,
Cyber Practice

Sources:

[1]https://www.coveware.com/blog/q3-2020-ransomware-marketplace-report

[2]Gallagher Drive™

[3]https://pdf.ic3.gov/2019_IC3Report.pdf

[4]1H20 Review of Trends in Ransomware and Doxing

[5]https://www.beazley.com/Documents/2020/beazley-breach-briefing-2020.pdf

[6]https://info.coalitioninc.com/download-2020-cyber-claims-report.html

[7]https://info.coalitioninc.com/download-2020-cyber-claims-report.html

[8]https://www.tessian.com/blog/biggest-gdpr-fines-2020/

[9]https://www.hhs.gov/about/news/2020/09/25/health-insurer-pays-6-85-million-settle-data-breach-affecting-over-10-4-million-people.html

[10]https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf

[11]https://news.bloomberglaw.com/privacy-and-data-security/facebook-wins-preliminary-approval-for-biometric-privacy-accord

[12]Advisen & Partner Re, Cyber Insurance — The Market View

[13]Gallagher Drive™