2020 saw the rise of several key trends in the cybersecurity space, exacerbated by the COVID-19 pandemic and an ever-increasing reliance on technology. As we head into the New Year, let’s look at some of the most pressing issues facing our clients into 2021 and beyond.

**Third-Party Vendor Risk**

There were a number of extremely high-profile cloud service breaches in 2020, most notably the [SolarWinds data breach](https://www.solarwinds.com/solarwinds compromises) and the [Blackbaud data breach](https://www.blackbaud.com/about-us). The effects from both these incidents trickled all the way down to the customers of those cloud service providers, generating greater concern about the risk of a systemic cyber event. These breaches also brought to light the limitations in transferring risks contractually through third-party vendors, especially if those vendors have not been properly vetted to ascertain the strength of their security and adequacy of their own insurance.

We are recommending much more thorough due diligence of outside vendors and businesses partners who would have access to sensitive data or systems. In 2021 and beyond, current market conditions have simply made businesses too vulnerable and the processes in place will have a direct impact on insurability, total cost of risk, and the availability of adequate insurance limits.

**Increased Regulation**

One of the [ballot measures](https://www.elections.oregon.gov/2020Ballots) that we had our eye on, Proposition 24 or the California Privacy Rights Act (CPRA), was passed, further expanding the California Consumer Privacy Act (CCPA). This is the most stringent privacy regulation to be enacted by a state thus far, and it could kick off another wave of regulations for other states. The CCPA and CPRA go beyond a company’s responsibilities following a data breach and place strict requirements on how businesses collect and store information in the first place. This is also the first US law to set a minimum threshold for statutory damages. This and other similar laws will help to protect consumers, but will certainly lead to a significant uptick in class action litigation and regulatory activity.
Ransomware

The number one trend that we have been dealing with in 2020 is the rise in ransomware attacks. This year saw a 125% plus increase in attacks with ransom demands regularly exceeding $1 million, regardless of the size of the business. Ransomware attackers have greatly expanded their scope, targeting companies of all sizes and within every industry, regardless of how much personal identifiable information they are able to exfiltrate from these companies.

The growing breadth and sophistication of ransomware attacks have dramatically changed the cyber security and insurance landscape, which has also had to cope with the overall digitalization of businesses. As companies become more reliant on technology as a result of COVID-19 and remote working, many have come to realize the importance of investing in cyber insurance and strong cybersecurity controls.

The result of all this is an extremely hard insurance marketplace. Carriers are seeing declining profitability due to these severe and increased attacks, and increasing rates by as much as 30% and we anticipate this trend will continue through 2021. Insurance carriers have responded to this market shift by being more discerning with clients, engaging in extremely thorough qualitative analyses on the merits and controls of every individual risk before determining their insurability and pricing.

Industry Outlook

There is unfortunately no airtight cybersecurity defense strategy to prevent ransomware attacks, nor a public policy intervention that might help mitigate the risks. Ransomware attacks, as well as increased privacy regulation will continue. The market for cyber insurance is changing in response to these ongoing issues, so too must business.

There are hard times ahead for the cyber market, but we have learned a lot about how to strengthen our clients’ defenses in 2020. We can move forward into 2021 knowing that we have the right tools at our disposal to mitigate exposure, ensure insurability, and reduce the total cost of risk for our clients.

Want to learn more?

Find me on LinkedIn, here.

Connect with the Risk Strategies Cyber Risk team at cyber@risk-strategies.com.

Email me directly at rrosenzweig@risk-strategies.com.

TAGS:
Cyber Liability