PROTECTING YOUR DIGITAL FOOTPRINT DURING UNPREDICTABLE TIMES

Most businesses today rely on technology to optimize customer experience, improve operational efficiency, and increase revenue, which means that cybercrime and cyber security risks have increased exponentially. COVID-19 accelerated digital business, but digital transformation without the proper cyber security controls and risk management programs in place only provides more opportunities for malicious actors to exploit cybersecurity vulnerabilities. Businesses both large and small are more exposed than ever before to data risks, and these are problems that are not going away any time soon.

Year after year, the World Economic Forum ranks cyber security risk as one of the top global business risks. **This is why:**

- **95%** of cybersecurity breaches are caused by human error
- Data breaches exposed **36 billion records** in the first half of 2020
- As of 2020, the average cost of a data breach is **$3.86 million**
- The Equifax breach cost the company over **$4 billion**
- On average, ransomware attacks cost businesses **$133,000**
- More than **77%** of organizations do not have incident response plans in place

Cyber security is becoming a greater business priority, and this means that companies are turning to cyber insurance to protect their assets. However, because the severity and frequency of claims continues to rise year over year, cyber insurers are taking a close look at how this trend is impacting their profitability. Recent losses, threat volatility, and lack of historical data create layers of unpredictability that make cyber insurers wary of providing coverage. Now more so than before, cyber insurers are very calculated in their risk selection and pricing. Insureds and brokers are now dealing with a hard market that makes it difficult to find underwriters willing to write their risk.

Additionally, most cyber insurance carriers now require companies implement supplemental cyber security controls, like multi-factor authentication, segmentation of data, network encryption, and data backup before deciding to provide them coverage. Oftentimes when companies do not have these critical controls in place, they also do not have enough time or resources to develop the cyber security measures that insurance carriers require of them before underwriting their risk.

Companies that need help navigating the complexities of the cyber insurance space can, and should, turn to experts who have long-standing relationships with underwriters and understand what they are looking for in a company's risk profile.

BRP's MiddleMarket group has proven success helping companies of all sizes get the coverage they need, even in a hard market. We leverage our deep industry connections to underwriters in the cyber insurance space and also provide in depth coverage comparisons, proposals, and webinars that help protect critical digital assets. Stay ahead of threats instead of waiting until it's too late.

BRP's MiddleMarket Group

AHT INSURANCE
A BALDWIN RISK PARTNER