Proskauer

Cyber Insurance Needs in the Pandemic Landscape

May 27, 2020

While most of society struggles to flatten the curve, treat the sick and restart the economy, regrettably, some bad actors have used the COVID-19 emergency as an opportunity to exploit vulnerabilities for personal gain. One of the key areas of increased exposure is cybersecurity. Companies should review their risk management and insurance arrangements now to ensure that they are properly protected in the event they become the target of cyber crime.

The rapid and unexpected onset of the coronavirus pandemic resulted in massive changes in the way we do business. The transition from secure office infrastructure to working from home on personal devices and home networks took place almost overnight, leaving gaps in data security. Add public anxiety over coronavirus health concerns and economic hardship, and it is difficult to imagine a more perfect storm of cyber risk.

Scammers have impersonated the U.S. Centers for Disease Control and Prevention, the World Health Organization and other health authorities. A Johns Hopkins coronavirus data map was used to divert users to malicious websites. Phishers are using coronavirus themes, such as governmental loan programs and fake charities, to trick users into turning over money and sensitive business information. Ransomware attacks are on the rise. And data thieves are targeting industries involved in COVID-19 medical and pharmaceutical research. Indeed, all businesses are at risk.

Insurance coverage for cyber events can be found in different types of insurance policies, including some traditional crime, general liability, and first-party property policies, as well as newer policies tailored to cyber risks. In recent years, the insurance market has begun offering broader coverage for key cyber risks such as social engineering, ransom, extortion, business interruption and data breaches. However, the coverage terms still vary considerably from one policy to another, which can mean the difference between payment of the claim or denial. Companies suffering cyber losses should also look to indemnity agreements and vendor contracts with their counterparties, and to additional insured status on policies issued to counterparties that may be liable for the breach.

Cyber policies are not one size fits all, as the cyber risks facing a particular policyholder can vary based on business sector, risk profile and other specific needs. Careful review and negotiation is therefore needed. Now is the time to review these insurance and contractual arrangements comprehensively to protect your company when it may be most vulnerable.

The bottom line is this: these are extraordinary times and you should not make any assumptions about your coverage. Details matter. Expertise matters. Let us know if we can help.

* * * *

Proskauer's cross-disciplinary, cross-jurisdictional Coronavirus Response Team is focused on supporting and addressing client concerns. We will continue to evaluate the CARES Act, related regulations and any subsequent legislation to provide our clients guidance in real time. Please visit our Coronavirus Resource Center for guidance on risk management measures, practical steps businesses can take and resources to help manage ongoing operations.

Related Professionals

- **John E. Failla**
  Partner
- **Nathan R. Lander**
  Partner