COVID-19 Crisis May Warrant Changes to Your Cyber Insurance Coverage

JONES DAY

COMMENTARY

JULY 2020

IN SHORT

The Situation: Cyberattacks have increased during the COVID-19 crisis as malicious actors have exploited network vulnerabilities resulting from remote work environments.

The Result: Many current cyber insurance policies may fail to provide complete protection for the risk of data breach, network shutdowns, and civil and regulatory actions created by these new network vulnerabilities.

Looking Ahead: Expanded remote work arrangements will remain with us for the foreseeable future. Corporate policyholders should review their cyber insurance programs and make modifications as necessary to cover the associated risks and defeat potential coverage defenses.

With the onset of the COVID-19 crisis, U.S. businesses were forced to rapidly expand their remote IT capabilities to allow employees to work from home. This process created new network vulnerabilities due to the proliferation of access points, increased reliance on personal devices, and erosion of central data controls. As a result, there has been an upsurge in cyberattacks in the last few months, and this trend will likely continue for the duration of the pandemic.

Cyber insurance plays a critical role in mitigating the business risk of a cyberattack. A well-crafted policy can protect a corporate policyholder from tens of millions of dollars of financial exposure resulting from a data breach. But many cyber policies may not adequately cover the emerging risks surrounding remote work environments, and potential modifications should be considered to obtain additional protections in the age of COVID-19.

Cyber Insurance Primer

Cyber insurance has been in existence for more than 20 years, first in connection with other lines of coverage, then as standalone cyber policies. But the market remains a challenging one for policyholders. There is very little case law interpreting cyber policies, and standardized policy language has not yet emerged. Despite the variation between policy forms, most cyber policies contain the following essential coverages:

- *Data Breach Expense,* covering standard breach response costs to retain attorneys and forensic investigators and to notify customers whose personal information has been compromised.
- *Privacy/Network Security Liability,* covering the defense and settlement of class actions and third-party claims.
- *Regulatory Claims,* covering legal fees to respond to government investigations, as well as civil fines, penalties, and settlements.
- *Network Interruption,* covering lost profits and extra expenses resulting from a network shutdown.

Cyber insurers also offer a range of optional coverages to address specific risks, such as ransomware attacks, data restoration, and payment card liability. The scope of coverage varies significantly between policy forms, and differences in policy wording may determine which losses can be transferred to the insurer.

> Businesses should consider modifying their cyber policies to address the emerging risks, with a focus on the specific wording of key policy terms that can make the difference between an insured loss and an uninsured loss.

Implications of the COVID-19 Crisis

Regarding particular risks surrounding remote work environments, some cyber policies may have coverage gaps or imprecise wording that insurers can exploit to argue against coverage. For example:

- There has been a sharp increase reported in two types of cyberattacks during the COVID-19 crisis: (i) ransomware attacks, where hackers use malware to encrypt a company's data, then demand a cryptocurrency payment to provide decryption keys; and (ii) fraudulent transfer schemes, where hackers send forged emails to targeted employees to induce them to transfer funds to offshore accounts. These events may not fall within the standard insuring agreements and often must be added by endorsement, and the specific wording of the endorsement could determine whether coverage is available.

- Many cyber policies include exclusions for negligent network security practices—which, of course, is contrary to the very purpose of cyber insurance. We have seen exclusions for delayed software patches, use of unencrypted portable devices, and design errors affecting network traffic capacity. Such exclusions can be highly problematic, particularly during COVID-19 when network IT resources are strained.

- The California Consumer Protection Act ("CCPA") took effect on January 1, 2020, coinciding with COVID-19's arrival in the United States. This statute, considered to be the nation's toughest consumer privacy law, imposes new requirements regarding data security practices, third-party sharing, and disclosure of collection policies. For many companies, CCPA compliance required costly investment in new data systems and processes. These burdens could not have come at a worse time for U.S. businesses, as they struggle with limited cash flow to maintain fluid and effective IT networks. Violations of the CCPA can result in civil claims, statutory damages, and regulatory investigations. It is important for corporate policyholders to ensure that their cyber insurance policies provide adequate coverage for these new regulatory exposures.

Plugging the Gaps

Given the rapid evolution of cyber insurance coupled with COVID-19 data security concerns, corporate policyholders should consider conducting a close review of their policies every renewal cycle to determine the adequacy of coverage. Expanded remote work arrangements will persist for the foreseeable future and, in some sectors, become part of the "new normal." Businesses should consider modifying their cyber policies to address the emerging risks, with a focus on the specific wording of key policy terms that can make the difference between an insured loss and an uninsured loss.

TWO KEY TAKEAWAYS

1. COVID-19 has required corporate policyholders to implement expanded remote work strategies that could become part of the "new normal" for certain business sectors. These strategies can increase the risk of cyberattacks.


Tyrone R. Childress
Los Angeles


Richard DeNatale
San Francisco

2. Corporate policyholders should review their cyber insurance programs, with the help of experienced insurance counsel, to assess the adequacy of coverage for the emerging threats created by the new digital work environment and minimize their insurer's ability to avoid coverage for cyber losses.

Craig M. Hirsch
Los Angeles