COVID-19: DOES YOUR CYBER POLICY COVER REMOTE WORKING CYBER RISKS?

Date: 18 May 2020

Cyber Insurance Alert

By: Jeffrey J. Meagher

Working from home has quickly become the new normal, but it may also be the reason your cyber insurer denies coverage for the next cyberattack. With most of the United States currently under or just emerging from some form of stay-at-home guidance, the number of people working remotely likely has never been higher. While work-from-home capabilities have allowed many companies to maintain productivity during the current global pandemic, those same capabilities may simultaneously increase your company's cyber risk and (at least according to your insurer) limit the protection provided by your cyber insurance policy.

COVID-19-RELATED CYBERATTACKS ON THE RISE

According to the U.S. Department of Homeland Security, malicious cyber actors are already taking advantage of the work-from-home environment by launching COVID-19-related phishing campaigns and exploiting publicly known vulnerabilities in remote networking software. For example, some cybercriminals are using an app that promises to provide real-time coronavirus tracking information to trick the user into providing administrative access to install “CovidLock” ransomware on their device. To create the impression of authenticity, cybercriminals may spoof sender information in an email to make it appear to come from a trustworthy source, such as the World Health Organization. In several examples, cybercriminals are sending phishing emails that contain links to a fake email login page. Other emails appear to be from an organization's human resources department and advise the employee to open an attachment. It may be months before we know how many of these attacks were successful.

THE DEFINITION OF “COMPUTER SYSTEM” IN YOUR CYBER POLICY

In the meantime, policyholders would be well-advised to review their cyber insurance policies and consider whether they have adequate coverage for cyberattacks in the current work-from-home environment. Most cyber policies provide coverage for loss that results from a “Security Event” (or some similar term) where that term is defined to mean the failure or violation of the security of a “Computer System.” While the specific definition varies from policy to policy, one common cyber form defines “Computer System” to mean:

computer hardware or software or any components thereof that are linked together through a network of two or more devices that are accessible through the Internet, internal network or connected with data storage or other peripheral devices (including, without limitation, wireless and mobile devices), and are under the ownership, operation or control of the Insured.

Other policies define “Computer System” to include hardware or software “owned by your employees and operated on behalf of you.” In addition, some policies define “Security Event” to include a failure or violation that results from the theft of a password from the “Insured's premises” or “Computer System.”

©2005-2024 K&L Gates LLP. All Rights Reserved.

DOES YOUR CYBER POLICY COVER SECURITY FAILURES INVOLVING PERSONAL COMPUTER SYSTEMS?

Any definition of “Security Event” or “Computer System” that provides coverage for security failures involving hardware or software under the “ownership, operation, or control” of the “Insured” or the theft of a password from the “Insured's premises” may be problematic (at least according to your insurer) in the current work-from-home environment, particularly if your employees are using their own personal laptops, smartphones, or wireless routers. Even a definition of “Computer System” that expressly includes hardware or software “owned by your employees and operated on behalf of you” could be problematic (again, according to your insurer) if the security failure occurs when your employee was using the hardware or software for personal activities. These issues may be further complicated by the fact that many cyber policies define “Computer System” to include the computer systems of service providers whose own employees may be working from home using their own personal laptops, smartphones, and wireless routers. That said, policyholders may be able to argue that they exercise some form of control over their employees' personal computer systems or that an uncovered security failure involving a personal computer system led to a covered security failure involving the policyholder's “Computer System,” so there may still be paths to coverage. Accordingly, no policyholder should simply accept a coverage denial at face value.

CONCLUSION

The recent, rapid shift to remote working and the corresponding increase in cyber risk involving personal computer systems may represent a significant new cyber exposure for many companies. Policyholders would be well-advised to review their current cyber policies to determine whether they have coverage for the remote working cyber risks identified above and take steps to address any potential gaps in coverage (e.g., policyholders may decide to limit or exercise some form of control over personal computer systems used for work purposes). Policyholders may also want to address remote working cyber risks with their cyber insurer at renewal.

KEY CONTACTS

JEFFREY J. MEAGHER
PARTNER

PITTSBURGH
+1.412.355.8359
JEFFREY.MEAGHER@KLGATES.COM

This publication/newsletter is for informational purposes and does not contain or convey legal advice. The information herein should not be used or relied upon in regard to any particular facts or circumstances without first consulting a lawyer. Any views expressed herein are those of the author(s) and not necessarily those of the law firm's clients.

©2005-2024 K&L Gates LLP. All Rights Reserved.