To Our Clients and Friends

Memorandum

May 20, 2020

Cyber Insurance Coverage in the Remote Working World

The recent mass shift to remote working caused by the global pandemic has provided an ideal breeding ground for both malicious cyber attacks and unintentional data security incidents. Intentional attackers have not only taken advantage of the chaos and fear associated with the pandemic, but they have also capitalized on vulnerabilities newly created by a displaced global workforce. In addition, the use of "home offices" as an employee's primary, rather than occasional, work environment introduces new technologies and behaviors that can lead to intentional and unintentional network compromises and data losses.

While robust and well-tested cybersecurity protocols and practices are always the first line of defense against such attacks, cybersecurity insurance has served as a critical tool for businesses seeking to mitigate the fallout from cyber and data loss incidents. However, companies must understand the extent to which their cyber insurance policies cover losses attributable to cyber attacks on employees' "home offices," as well as those associated with security gaps created by the sudden shift to remote work. In many cases, depending on the nature of the existing coverage, certain losses may not be insured, and companies may need to expand or modify their existing cyber policies.

Find and Mind the Gaps

Most companies will have some degree of coverage for losses associated with remote work, given that even before the pandemic, companies made use of remote login capabilities for after-hours work, work travel and the other off premises needs of their workforces without any special insuring agreements. In fact, many cyber insurance model forms do not reference a worker's physical location at the time of an incident, and some even go a step farther and provide coverage for losses occurring anywhere in the world.

Nonetheless, the scale and speed of the workforce displacement triggered by the pandemic has generated new attack and loss vectors not previously contemplated. For instance, more employees now work remotely on personal, rather than company-issued, devices. Relatedly, many more employees now access company systems outside the confines of a virtual private network, and use insufficiently secure hardware, such as home wireless routers. In an effort to keep up with workloads, employees will undoubtedly come up with creative workarounds to access company systems or work on devices accessible by multiple household members. The end result of these perhaps understandable behaviors may be a material departure from the company's cybersecurity and data privacy policies and procedures, as well as the representations made by the company to its insurance carrier.

Along these lines, two aspects of a typical cyber insurance policy present the greatest potential gaps in insurance coverage when supporting a remote workforce: (1) whether the company owns or operates the

affected network, device and/or systems at issue in the incident; and (2) whether the incident stemmed from a departure from the company's information security and data privacy policies and practices, as represented in its coverage application.

Whose Network, Devices or Systems Caused the Loss?

One of the biggest coverage questions for an incident arising from remote working is whether the "network" impacted is included within the policy language. For example, imagine a scenario where a ransomware attack on an employee's home computer results in the loss of confidential company information the employee had previously downloaded and saved on that computer. Imagine next that the compromised materials contain information that allows the attacker also to penetrate the company's own network. Whether the company has coverage for such incidents may depend on whether the policy's definition of "network" is limited to software, hardware, devices and other infrastructure *owned, operated, controlled or leased* by the company.

Some policies are silent on who must own or control the network for coverage to be triggered, and simply describe the component parts of the network that are covered. Other common definitions of "network" include a specific requirement that the network be "owned," "operated," "controlled" or "leased" by the company itself. A broader version of that definition also covers each "Insured Person," which can include executives and officers and sometimes employees.

While the definition of Insured will always be crucial to coverage, it is particularly significant to remote working, where employees may be working entirely or partially outside the confines of the company network and devices. In such a scenario, an insurer might argue that a cyber policy that limits coverage to infrastructure *owned* by the company excludes coverage for an incident arising from a remote employee's use of a personal device, even where that device provides a vector to attack the company's "network" because the use of the personal device was the proximate cause of the company's losses.

Compliance with Cybersecurity and Data Privacy Policies and Procedures

Cyber coverage for incidents occurring during the pandemic may also be complicated by the representations made by the company in obtaining or modifying its policy. Typical cyber insurance applications require a prospective insured to provide detailed information concerning its information and data security policies and procedures. Such applications often include questions about (i) policies and practices related to password and anti-virus protection and the encryption of laptops, smartphones and tablets; (ii) measures taken to secure remote access of the company's network, including the use of multifactor authentication and virtual private networks; (iii) information concerning the number of remote-use devices; (iv) the configuration of wireless networks to protect against unauthorized access; (v) restrictions on physical access to computer systems and sensitive paper records and employees' ability to remove data via network endpoints; and (vi) the identity of the internet service providers used to access the network. The response to each one of these questions may be materially impacted by new practices – both formal and ad hoc – taken up by a company's workforce in light of the pandemic.

And while it is true that representations required in insurance applications are generally only required to be true as of the time made, an update may be required at different points during the life cycle of an insurance program.

- Some applications require the insured to describe any expected changes to operations over the ensuing twelve months. Companies with such policies should closely examine their responses to such questions to see whether they were true at the time.

- Nearly all applications require the insured to update changes to the representations made between the time the application is completed and the time the policy is issued. To the extent a company applied for insurance or renewal of a policy before the pandemic, changed circumstances may require an update to the representations made in the application before the inception of the insurance policy.

- While policies incorporate by reference representations made in applications, others may require an insured to update those representations where insurance risk has increased. A mass transition to remote working in the midst of a global pandemic may require such an update.

- Short-form renewal applications often focus on whether there have been any material changes in the company's policies and procedures since the prior application. Any renewal during the pandemic must prioritize a review of the company's policies and procedures concerning remote working.

- The policy itself may obligate a company to ensure that its employees adhere to its policies and procedures in order to claim coverage for an incident. For example, a "Minimum Required Practices" exclusion can be used to deny coverage for losses to the extent the company failed to follow information security practices at least as robust as those disclosed in its insurance application.

The consequences for not following the policies and procedures represented in a company's applications or incorporated by reference into the policy can be severe, depending on the law of the jurisdiction governing the policy – from complete rescission of the policy to a reduction in coverage.

Recommendations

There are a few steps companies should take now to maximize coverage for remote working-originated incidents that are sure to arise.

1. Cyber insurance policy writing is still in its infancy, with highly customized insuring agreements and endorsements. As a result, there can be considerable variance in the terms of the coverage offered by different insurers, and the interpretation of cyber policy language has not been sufficiently tested in litigation. Companies should take time to speak with counsel and brokers to discuss hypothetical coverage disputes.

2. A company's coverage may include loss prevention and mitigation services that allow the company to consult its carrier before a cyber incident or data breach has occurred. Once the company has thought through the potential consequences of its remote working risks, it should take advantage of such services to engage in a dialogue with its carrier. While that dialogue will not result in changing the scope of existing coverage, absent modification, it may assist the company in making changes to its policies and procedures to bring remote working practices within scope as best as practicable.

3. It is not too late to negotiate for modifications to coverage. Indeed, some policies give a policyholder the right to propose policy amendments to the extent that insurance risk has

increased or changed during the policy period. Similarly, companies should look to renegotiate, where appropriate, when the policy comes up for renewal.

Widespread remote working appears here to stay, even after the worst of the COVID-19 pandemic subsides. Many companies have found that the transition to remote work in itself has not significantly impacted productivity, and will undoubtedly choose to keep at least some portion of their work forces remote going forward. In light of these factors, companies should revisit the scope of their cyber coverage through a review of potential policy issues and by formulating a customized policy that meets their needs and operational risks.

* * *

Authors:

Una A. Dean

Michael A. Kleinman

Jasen T. Fears

This memorandum is not intended to provide legal advice, and no legal or business decision should be based on its contents. If you have any questions about the contents of this memorandum, please call your regular Fried Frank contact or an attorney listed below:

Contacts and COVID-19 Task Force Co-Heads:

Una A. Dean	+1.212.859.8851	una.dean@friedfrank.com
Steven M. Witzel (Co-Head)	+1.212.859.8592	steven.witzel@friedfrank.com
Gail Weinstein (Co-Head)	+1.212.859.8031	gail.weinstein@friedfrank.com
Jennifer A. Yashar (Co-Head)	+1.212.859.8410	jennifer.yashar@friedfrank.com
Joshua D. Roth (Co-Head)	+1.212.859.8035	joshua.roth@friedfrank.com