

INSIGHTS

## Does Work-From-Home Work for Your Company's Cyber Insurance?

January 19, 2021

By: [Vincent E. Morgan](#)

The start of a new year is always a good reminder to take some time to review key areas and assess whether changes are in order. There are many examples of this both personally and professionally, but a company's insurance program is certainly one on the business side and cyber insurance is at the top of that list. As many employees continue to work remotely, and some may do so permanently, it is important to monitor how this trend affects cyber insurance.

Cyber policies can insure against the destruction of, or loss of access to, computer networks, including response costs and other damages caused by cyberattacks and other intrusions. Like any other insurance policy, it is critically important for insureds to understand their rights and obligations under both the policy language and applicable law.

What is different for 2021 and beyond is the impact that work-from-home may have on the attestations many cyber policies require insureds to make about network security issues. These are generally fairly standard, and address issues such as encryption, backups, and access protocols. But they were designed for a world where most network access happened in controlled workplace environments that were easier to protect.

As COVID-19 drove a massive transition to work-from-home, companies have been addressing these issues to some degree. Throughout 2020, many companies made significant progress enhancing the security of their remote workforce by educating workers on basic but important steps like protecting Wi-Fi connections, updating software regularly, and using multi-factor authentication. Even with that progress, however, work-from-home can still limit corporate security departments' ability to monitor network traffic, secure connections, ensure updates are installed, and maintain the physical security of devices and confidential information—particularly where employees are not required (or able) to use VPN-level security.

While overall security measures for remote working likely improved during 2020, corporate policyholders still need to consider the impact this transition may have as cyber policies come up for renewal, or as some companies buy them for the first time. Coverage may depend on ensuring that the attestations remain true, or are modified as necessary.

Other aspects of cybersecurity also warrant this same review, such as the area between a covered cybersecurity incident and more generalized financial fraud. Social engineering schemes—where criminals send emails and make phone calls that appear to come from known

sources making legitimate requests, often for the transfer of funds—can fall into a coverage gap. The criminal may breach email or other corporate network resources to conduct reconnaissance and enable the scheme, but often the financial loss results from a deceived employee making an authentic request to a financial institution to transfer funds. This fact pattern may not be covered by cyber policies despite the fact that the loss involved a cybersecurity incident. Further, incidents possibly linked to state-sponsored actors may fall under common “hostile or warlike action” exclusions,” which are ripe for coverage disputes given the difficulty in attributing the source or motivation of cybersecurity incidents.<sup>1</sup>

As work-from-home continues to be prevalent and the broad array of cyber threats constantly evolves, it is more important than ever to have a coordinated approach to these issues through the company’s risk management, IT and legal departments as well as outside coverage counsel on these issues. That can identify any corrective actions that need to happen in order to minimize the risk of a cyber incident to begin with, and maximize the chance for coverage if one does happen.

---

<sup>1</sup> See, e.g., the ongoing litigation between Mondelez and Zurich about whether a ransomware incident triggered a war exclusion in Mondelez’s policy. *Mondelez Int’l, Inc. v. Zurich American Ins. Co.*, No. 2018L011008, 2018 WL 4941760 (Ill. Cir. Ct., Oct. 10, 2018).