It’s become clear as the coronavirus outbreak accelerates that it will impact nearly every business in some way. Leaders are working to determine how operational hiccups, added costs, and lost sales will affect their organizations, and how to mitigate the impacts.

What about cybersecurity? Are we in a unique threat environment?

We’ve already discussed how attackers are leveraging the natural desire for official information to launch phishing attacks, so in at least one sense there’s an elevated threat of intrusion. But when considering security posture, it’s not all about the external threats. Even if threat activity was completely unchanged by the coronavirus situation, a company’s overall risk could still be adversely affected by factors that relate its ability to protect itself and respond to an incident.

Let’s look at a couple of ways that could play out for your clients.

**Every remote worker is a variable**

First, take the influx of remote workers. Some businesses are already well equipped for remote work, with workforces that are accustomed to the security measures. Others aren’t.

There are well-understood methods to ensure that a remote workforce can replicate the security environment of an office, using VPN or remote desktop technologies. The problem is that these environments are like any other aspect of the security apparatus: they can be complex; they require adherence to best practices on the part of users to maximize safety; they must be diligently set up and provisioned; and they can harbor software vulnerabilities to keep up with and mitigate.

In other words, it’s not a utility where you can flip on a switch and get safe access.
Will a company rushing to equip its workforce properly configure its VPN to replicate the security of its in-office perimeter network? Will its employees find "shadow IT" workarounds because of the difficulty of using certain systems? Or worse, will the company eschew a VPN or other measure altogether, allowing for unencrypted access from home or public networks, in the name of expediency?

The wrong answer to any of these questions would represent a security gap that had previously not existed, and an opportunity for any attacker who discovered the soft spot. Moreover, even with a well configured, properly rolled-out remote environment setup, a fully remote workforce means that that system has suddenly gone from a business-enhancing technology to a critical point of failure, where an outage could lead to substantial lost productivity or business interruption.

Then you must consider how a worker outside of the office could expose data in a more physical sense. This could mean revealing passwords to a lurking over-the-shoulder looker at a coffee shop, having an unencrypted laptop stolen, or divulging information verbally while on the phone when they think they are alone. These factors all exist today for any business that has employees on the road traveling, or working remotely. But you can multiply any of these low-percentage risks by hundreds or thousands of workers in a fully-remote scenario — especially with those cabin-fevered remote workers seeking new environments to be in.

**More drastic scenarios: not off the table**

While we’re not there yet in the U.S., restrictions on movement and gatherings could come into force. In an even worse scenario, the outbreak could become so widespread that meaningful numbers of employees cannot work, even remotely, because they are sick. This kind of chaos has downstream implications for cybersecurity as well.

Attackers will seek any soft spots they can find, and businesses dealing with a severe outbreak in their area will be much more likely to cut corners. If much of the IT staff is off-site or too sick to work, what happens to the backlog security maintenance items, like software patching? Or to the business’s cyber incident response capacity?

If that business happens to be an IT vendor for other businesses, those weaknesses are extended to thousands that rely on it for basic processes. These are seemingly drastic scenarios, but the idea of restrictions on movement within a country like Italy would have sounded laughable a few weeks ago, and yet here they are.
What your clients can do to mitigate risk

One piece of unique advice given the situation would be to test out remote access systems with a “trial” day where everyone works from home, as a test, before it’s mandatory.

Otherwise, vigilance is the name of the game. Not many of the pieces of IT security advice that existed a few weeks ago have changed based on the outbreak; it’s about a business’s wherewithal to continue following them. Introducing 2-factor authentication for applications. The use of VPNs for remote access. Proper system hygiene for things like closing unneeded open ports and patching older software. These all applied before, and do so now.

All that, and transferring risk. If you’re a broker you don’t need to be reminded of the insurance angle, but it bears repeating that the incident response planning and post-breach services that are available to help insureds during a cyberattack could be particularly helpful if their team is stretched by the circumstances on top of an incident.

You can learn more about cyber risk in some of our recent content at www.corvusinsurance.com/news-and-insights.