COVID-19, Remote Working, and Cyber Attacks

By Andrew Armstrong

Amid the economic crisis brought on by the COVID-19 pandemic, many small businesses are devoting most of their attention to finances — and with good reason. The disruption caused by the pandemic threatens their very existence.

So, the questions insurance agents are hearing most often these days from small-business owners are:

1. “Am I covered for business interruption caused by the coronavirus?” (It depends on the language in the policy.)
2. “Am I eligible for PPP funding?” (See the conditions for the Payroll Protection Program on the coronavirus.gov website.)

But in the rush to secure funding to keep their operation running and their employees on the payroll, some businesses are paying too little attention to another potentially fatal risk: cyber-attack.

With unprecedented numbers of people working remotely due to the pandemic and more business than ever being transacted online, cyber criminals are recognizing vulnerabilities and exploiting them. As noted in the recently released document ***Warning: Cyber Liability — Increase Risk with COVID-19***: "Experts are projecting a **30-40 percent increase in cyber-attacks** during the novel coronavirus pandemic. This is primarily due to hackers exploiting the vulnerabilities associated with this crisis, especially those arising from employees working from home. In situations such as these, companies need to reexamine their network security infrastructure and Cyber Liability Insurance program."

Productivity vs. Security

While seeking information on financial assistance and insurance coverage, business owners have another priority that may compromise their cyber security: keeping their remote workforce as productive as possible.

"What's happening on the cyber security side is that people's guards are down," Asaf Lifshitz, CEO of Massachusetts and Israel-based Sayata Labs, tells the publication Insurance Business America. "Cyber security almost always comes at some degree of conflict with productivity, and all of a sudden [as a result of the coronavirus] there's this massive shortage of productivity. Companies need to be able to transact business, now that their employees are working from home and they're already taking a hit.

"In times like these, IT managers have to make compromises. Ideally, we'd like our employees to log in via a VPN, or to conform to whatever standards we put in place before. Now, it's much harder to enforce. If we insist on doing it, productivity will take a bigger hit, and so those constraints are relaxed a little bit — and that's what I mean when I say guards are down from a pure cyber security perspective."

Zoom bombs, Slack attacks and other trending threats

The Conversation website explores the risks of using popular online collaboration tools such as Zoom and Slack in its piece *Working from home risks online security and privacy— how to stay protected.* The piece includes these risk management tips:

- Be careful what you post publicly. Check that there is no potentially sensitive information in it. Once it's published online, it's there, forever.
- Check recent security and privacy reports about online collaboration tools before using them, and if in doubt, consult your employer. These tools can have access to details about your devices, your data and your video and audio conversations. The Electronic Frontier Foundation is a good source.

- Protect your devices. Install anti-virus software, update systems and apps, implement multi-factor authentication (so that multiple pieces of evidence are needed for someone to use your login, such as username and password and a text message), and be on the lookout for phishing scams.
- Zoom Bombing and other forms of hijacking meetings can be prevented. Share meeting links with only invited parties. Configure Zoom to only allow the host to share screen, as appropriate. And disable file transfers to stop trolls sharing viruses to all attendees.

The importance of cyber insurance

While good risk management is always advisable, it's also true that cyber breaches are inevitable. As I've written before, "Because no business is immune to cybercrime, it stands to reason that every business should protect itself with cyber insurance. Competitive pricing among the broad array of carriers offering coverage further contributes to the value of a cyber policy."
