8 Reasons to Modernize
Insurance Information Mgmt
w/ Nuxeo's Chief Transformation Officer
+ Perficient's Director of Financial Services
COMPLIMENTARY WEBINAR
Sponsored by
nuxeo

INSURANCE JOURNAL

View this article online: https://www.insurancejournal.com/news/national/2020/03/13/561054.htm

Coronavirus Work-from-Home Response May Expand Cyber Risk

As U.S. employers ask employees to work from home to avoid exposure to coronavirus, they may be exposing themselves to another kind of risk: Cyberattacks.

Aon recently issued an advisory cautioning employers to take steps to ensure that work-from-home employees can connect to secure remote networks.

“Any time you’re taking about employees who are not used to working from home, who may not have the correct cybersecurity posture, a virtual private network is critically important and having two-factor authentication is critically important,” Aon Senior Vice President Stephanie Snyder said in an interview.

Work-from-home employees may be especially vulnerable to phishing expeditions. Aon said there have already been reports of phishing emails being sent out posing as alerts regarding COVID-19, which is the specific coronavirus that has infected an estimated 100,000 worldwide. A phish is used to implant malware in a computer that can give hackers an opportunity to demand a ransom or steal data.

“In an environment where people are stressed and hungry for more information, there is a lack of commitment to security best practices,” the Aon report says.

Snyder said telecommuters may be tempted to sneak off to Starbucks to work from their laptops. She said that could expose all of the records on their computer to a potential hack. She said employers need to have strict security protocols in place to avoid such exposures.

Aon said businesses throughout Asia has activated business contingency plans that allow or instruct employees to work from home. Those contingency plans followed the virus to the West Coast of the United States last week.

King County, Washington, which has had the worst outbreak in the U.S. so far, last week asked all of its 2.2 residents to work from home if possible. The county Health Department said 51 cases had been confirmed as of late Friday, with 10 deaths.

In California, Apple on Friday asked its 12,000 Silicon Valley employees to work from home, Reuters reported. Facebook and Google also advised employees to work from home if possible to avoid the risk of spreading the virus.

Those tech giants presumably have adequate security in place for their telecommuting employees. That may not be the case for smaller businesses that have all of their security apparatus wired in only to the home office, said Rajeev Gupta, co-founder of Cowbell, a Pleasanton, California-based cyber insurer that launched in January.

Gupta said the complete lack of a virtual private network is one of the most common cybersecurity mistakes that he’s seen among small employers. Another mistake is having a VPN but making it accessible only on one server or an inadequate number of servers to handle the load created by employees trying to gain access from remote locations.

“You have to scale the infrastructure according to need,” he said.

Like Snyder, Gupta said employees connecting to public servers are also a hazard. He said many people who use their computers for work will log into Wifi at a coffee shop or at a hotel without a second thought. Without a VPN, “the hackers are going to have a field day,” he said.

CyberScout, a cybersecurity firm based in Scottsdale, Ariz., issued a bulletin on Feb. 27 warning employers to beware of phishing scams and ransomware.

“It all comes down to access points,” CyberScout Chief Executive Officer Jennifer Leuer said in a prepared statement. “For every WiFi network that an employee signs on to, they are creating an additional access point for hackers to infiltrate your business systems. The danger is even greater if employees are using public WiFi.”

CyberScout suggested these tips for securing business data:

Set up a virtual private network, and be aware that some are better than others. The network should include multi-factor authentication.

Require employees to use private WiFi. If employees need to work from hotels, conference rooms and other public places, require them to use a mobile hotspot (such as those available through a smartphone) to access a secure connection.

Upgrade password requirements to require more complex and lengthy passwords and regularly change passwords — up to once a day if the culture will allow it.

In a telephone interview, Leuer said many small and mid-sized employers that have not paid much attention to cybersecurity are taking a closer look now because they are concerned employees will have to work from home.

“You never want to see a crisis go to waste,” she said. “Unfortunately, that’s what’s getting their attention.”

More from Insurance Journal

Today's Insurance Headlines | Most Popular | National News