COSMOS
Navigate the Compliance Universe

Report on Supply Chain Compliance Volume 3, Number 7. April 02, 2020
Cybersecurity threats take advantage of crisis

By Sascha Matuszak

News has trickled out[1] regarding new phishing attempts named after the coronavirus and an uptick in attacks. A crisis, followed by a lockdown, is an optimal time for hackers to infiltrate systems, establish control over vulnerable networks and demand ransom.

The danger lies not just in a lack of attention on cybersecurity while communities are dealing with the virus, but also in the fact that millions of people will be working from home, using a variety of patchwork systems and devices to maintain contact with offices and colleagues. Although no major attacks have been detected—aside from the aforementioned email phishing scam, which used the World Health Organization's name—now is the time to patch networks; establish standard, safe protocols for remote work; and train people on basic cybersecurity.

1 Naveen Goud, "Coronavirus and Email Phishing scam and Cyber Attack on WHO," *Cybersecurity Insiders*, March 2020, https://bit.ly/2WI2how.