industry victims. "No industry is immune," said Tony Sardis, partner and president of Withum Insurance Advisors. "Cybercrime takes on many different forms, from ...

Nov. 06, 2018

Cyber fraud in every industry not only exists but is thriving despite continuous efforts to minimize such risks, according to the professionals in WithumSmith+Brown (Withum) PC's Cyber and Information Security advisory group. Cybersecurity and ransomware attacks have become more amplified, rendering every business – large or small – a target for cyber attacks.

"Every business in every industry has an over-abundance of the two things cybercriminals are after – information and money," explained Joe Riccie, partner, market leader of the Cyber and Information Security Services Group. "There is a lot at stake, which is why business entities, from small privately owned companies to large publicly held corporations, have become even that more vulnerable and cybercrimes have become more common."

It is the speed at which today's transactions occur – thanks to a highly distributed mobile workforce, smart technology and wire services – unlocks a newfound level of exposure, according to Riccie.

"Criminals are focused on valuable company data, information about each of the parties (employees, clients, third-party vendors) and an entry point into the financial institutions/banks involved in any type of transaction," he said. "Once this information is accessed, hackers take it one step further to gain entry to personal account information that is then sold on the dark web or to other more sophisticated cyber criminals."

Robert Egan, a partner with Archer Law, urges cyberattack victims to own up to the

employees."

To protect one's company, employees, clients and third-party service providers, Sardis urges all businesses to implement certain strategies and tools to combat cyber fraud and promote cyber resiliency. He also has the following suggestions:

- Acquire cyber insurance from a reputable company for all business activities
- Require cyber insurance from your subcontractors and vendors
- Report any breaches to the insurance company immediately upon discovery

Rob Kleeger, founder and managing director of Digital4nx Group, Ltd., also advocates for employing certain password and authentication practices. "From encouraging longer pass phrases of at least 12 characters to utilizing password management tools such as LastPass, KeePass and Dashlane and enabling two-factor authentication whenever available, it is advisable to never use the same password on more than one site," he explained. "It also is advisable to encrypt devices that store PII or confidential data."