BUSINESSES SHOULD CONTINUE TAKING HEED WITH CYBERSECURITY IN THE WORKPLACE

David B. Rounds is the author of the book Breathe Easy: How Just ONE Cyber Attack Can Damage Your Business Beyond Repair...And What You Can Do NOW To Stop It. He is also CEO of NetEffect in Las Vegas, an award-winning, managed IT service provider that has spent over two decades as a trusted partner and expert in developing business technology and cyber security preparedness for small and midsize businesses.

By David B. Rounds, CEO of NetEffect

Cybercriminals continue to seek new ways to attain valuable personal and business data, as we have recently seen with the MGM and Caesar's attacks. As businesses continue to open their doors or grow, it is crucial to be savvy and implement methods to prevent online hackers.

Listed below are some essential steps and actions businesses and organizations should consider to enhance their cybersecurity and minimize the likelihood of future data hacks:

- It's vital that businesses keep spyware, malware, and other viruses off of their network. Cybercriminals always find new ways to access networks through normal daily activities, so have a solid, centralized, and alerting endpoint protection program installed. Employees should be strongly discouraged or barred from downloading programs such as screensavers, emoticons, peer-to-peer software, music files and similar programs. A single piece of malware installed on any of those types of programs can ruin an entire computer network.

- If hackers are determined to gain access to your network, they have more options than just hoping an employee clicks on an email attachment. Ensuring your network has up-to-date security patches and virus definitions is crucial. Also, business owners should install a strong firewall.

- Training employees on how to spot and avoid potential hacking efforts is essential and can help avoid costly repairs or replacement of your network. Employees should be given training in Best Practice use of all electronic devices and how to spot potentially malicious emails and other commonly used methods of infiltrating a business' network.

- Passwords are critically important for a secure network. Always remember, 'the longer, the better.' Network users' passwords should include at least one special character, one number, and both uppercase and lowercase letters.

- Use Advanced Email Security. Free email security that is provided with G-Suite or Office 365 does not offer sufficient security for your network. You must purchase upgraded network security. The extra cost is minimal compared to the potential cost to your business if it is hacked.

- One of the most hostile forms of cyberattacks is ransomware, in which a hacker locks up your files and holds them for ransom until you agree to pay a fee. Making sure your files are backed up will give you an alternative to paying cybercriminals to retrieve your data. Backing up files also protects your business from losing data due to employee error.

- Obtaining cyber liability/fraud insurance is a must. Even when it seems like a minor data breach, it can result in legal, forensic, and public relations costs that run into tens or hundreds of thousands of dollars. Insuring against these types of costs is necessary.