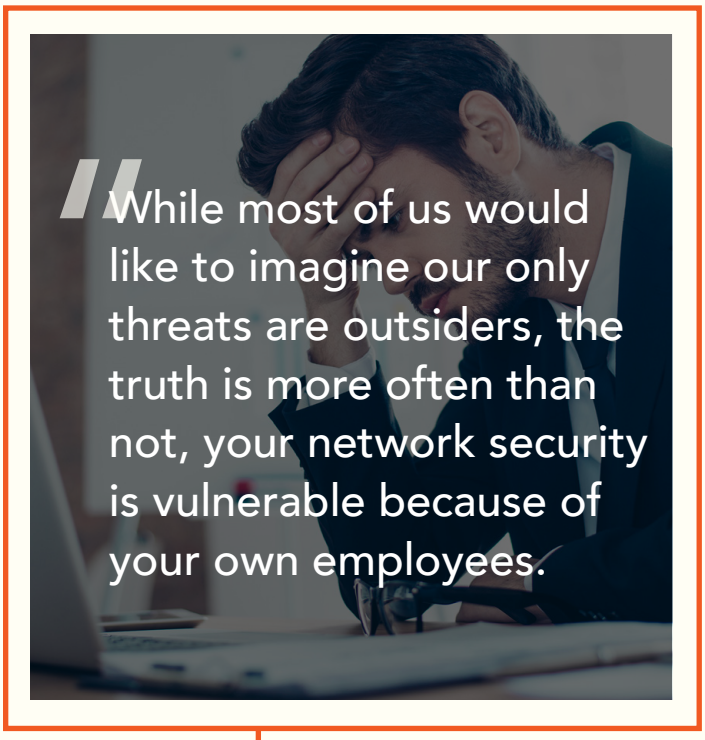
AFFINITY IT GROUP

www.affinityitgroup.com

THE NETWORK THREAT IS COMING FROM INSIDE THE HOUSE



LET'S TALK **STATISTICS**

You and your nine friends each own a business. Throughout the year, each business owner faces one network security problem. Six of you can look throughout your own office building and find the source of the problem sitting in one of your comfy desks.

While most of us would like to imagine our only threats are outsiders, the truth is more often than not, your network security is vulnerable because of your own employees.

Among 874 cybersecurity threat incidents, as reported by companies to the Ponemon Institute for its recent 2016 Cost of Data Breach Study, 568 were caused by employee or contractor negligence; 85 by outsiders using stolen credentials; and 191 by malicious employees and criminals.

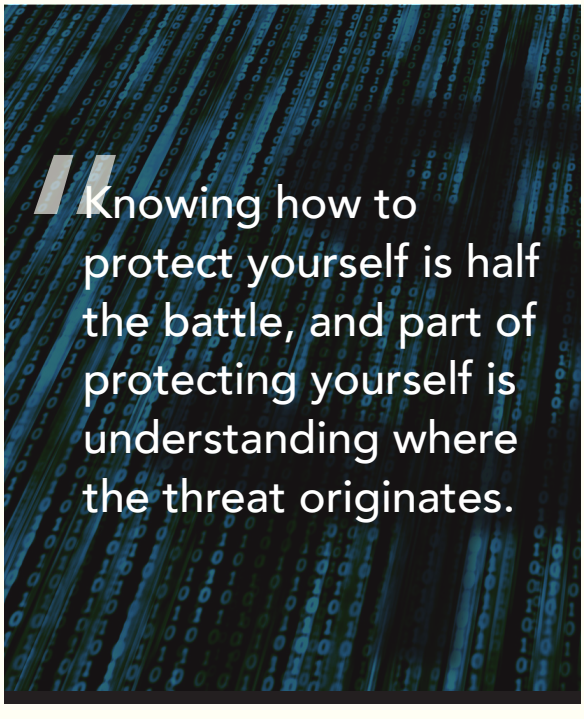
THE INSIDE **JOB**

The stories of big time hacking groups infiltrating networks and exploiting sensitive information are few and far between. Stories of Tom from accounting opening an email attachment that unleashes malware havoc on the company network are quite common. Tom might not have meant any harm, but due to his ignorance or lack of training, you've got a pretty big problem on your hands.

DON'T FIRE TOM; **TRAIN TOM**

Now that you're thinking about cybersecurity threats a little differently, how do you protect yourself? While some insider threats are caused by malicious users, many are caused by a simple lack of training. There are a few things you can begin doing to help protect your business from the inside, out.

1. Know your employees and what they can access. By remaining familiar with the individuals filling your office space, or working remotely, you can have a better idea of the duties each worker performs and the level of access to your critical and sensitive business information they require. Perhaps Tom in accounting doesn't need to be granted permissions to certain shared drive folders. If your employee can't access it, it will be much tougher for a malware attack to be successful.



2. Train your employees. The majority of your inside threats are not caused by malicious individuals, but unwitting ones. With proper training, you are much more likely to house an office of workers who won't become victims.

3. Monitor your staff's systems updates. Most people are annoyed by the constant security updates on their computers, and many don't understand the importance of adhering to their schedule. Your IT lead should be checking to make sure each computer user in your office remains current on security updates and alert for suspicious activity.

CONCLUSION

Knowing how to protect yourself is half the battle, and part of protecting yourself is understanding where the threat originates. It should be at least somewhat comforting to know that preventing an attack is easier than you might have guessed. With proper training of your staff and active monitoring, you can give yourself the best opportunity to avoid the mess of lost data or exploited information.

If you're ready to take your network security to the next level, contact Affinity IT Group today. We'll make sure Tom doesn't crash your system.

AFFINITY IT GROUP

www.affinityitgroup.com

Phone
+800.627.2214

Email
Info@AffinityITGroup.com

Address
6920 Spring Valley Dr
Suite 106
Holland, Ohio, 43528