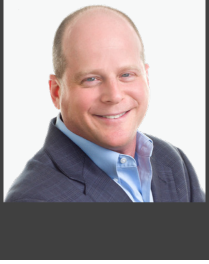
Season 3 | Episode 63

# 5% Don't Think Cybersecurity is Important. Why Risk It? Take Steps to Protect Your Business



Gene Marks

CPA, Columnist, and Host

**Gene Marks:**
Hey everybody, and welcome to this week's episode of "On the Mark". My name is Gene marks, and thanks for joining me, where I will look at some news that impacts your small business and mine and give you some advice.

Speaking of advice, if you have any topics, guests that you would like to suggest for this podcast or other THRIVE podcasts, please visit us at our page payx.me/thrivetopics. That's P-A-Y-X dot M-E/thrive topics.

All right, the news this week has to do with cybersecurity. There is a new survey that was published this past week by CNBC and SurveyMonkey, and you know what, the news for small businesses is not so great. The survey looked at more than 2,000 small-business owners — it looks at it every quarter — and in this latest survey, it found that just 5 percent of small-business owners reported cybersecurity to be the biggest risk to their business right now.

OK, I mean I realize inflation is a big risk and finding good employees is another risk. But only 5%? That really is really interesting that that number is so low. The smallest of small businesses are the least concerned about cyberattacks: 33% of owners with zero to four employees are concerned about experiencing a cyberattack within a year compared with 61% of small-business owners with 50 or more employees, which is really something that just concerns me, as well.

Some of the other data for you, when people are looking at their risks of cyberattacks in their business, their preparedness varies from industry to industry. Some say that they have confidence their banks are providing enough security. Others say their healthcare providers and email providers are covering and dealing and taking care of security issues pretty well.

But it really goes well, well beyond that, guys. When it comes to cybersecurity, when I try to talk to my clients or people that I like to write about that have suffered a cybersecurity issue, a lot of people are unwilling to speak because it's not something you really want to advertise.

So, in my opinion, whenever you read about the data of small businesses that have bene affected by cybersecurity attacks, I believe they are generally underreported because the media is going to focus on larger companies and not necessarily smaller businesses. And, again, small businesses themselves are not going to be jumping up and down to report that they think cybersecurity has become an issue for their business.

So, just remember, like only 5% of small-business owners reported cybersecurity to be their biggest risk to their business right now. I mean, it's a big risk and let me tell you why. If you get impacted my malware or ransomware attacks where security fees can lock up all your files and demand money paid to them in digital currency for them to give you a key to unlock those file, that cannot only disrupt your business for days or even weeks, and in some instances, it can cause your business to shut down. So, you have to be very much aware of cyberattacks.

One other thing you should be aware of, too, is — with everybody working from home since April of 2020 when the pandemic started — cybersecurity attacks have increased 300 to 400% because they are going after us when we're working from home, as well, and that's another concern we have to aware of.

So listen, as we're emerging from the pandemic and as a lot of us are still having a lot of our employees working from home or having hybrid /remote-work arrangements with them, cybersecurity is going to continue to be a really big deal, and I don't think that the 95% of the people who don't think this is a priority for them, well, I think they are wrong.

I do think that inflation and that labor shortages are going to be an issue that will pass, but cybersecurity is going to be with us for a long time.

So, let me give you some advice, let me tell you what my smartest clients are doing this year. They're spending a little bit of money on security. They're hiring IT firms that specialize in security to help them. And what these IT security firms are doing is they are zeroing in on their work-from-home employees. I mean, sure, you get the security software and the backups, but there are a lot of other things that employees should be doing if they're working from home or elsewhere that you need to have an IT firm in the middle of.

IT firms that are working with my clients are doing this:

No. 1: They are training employees because the biggest perpetrator of IT security attacks is our own employees and ourselves, as well. Sometimes we click on the wrong link or we don't recognize a phishing email or something with malware attached to it because we're not used to seeing it all the time.

Well, if you hire a good IT firm, they will provide some training for you and your employees, at least on a quarterly basis, to make you all aware of what things to avoid, things to have your radar up for a potential malware attack, emails to look for, or nefarious websites. so, get training. That's No. 1.

No. 2: A good IT security firm will get involved and reconfigure the home routers of your work-from-home employees. Let's face it, a lot of us are still using the passwords that came with it out of the factory, and a lot of us don't really do much security for our routers at home. And, yet, routers are so easily compromised that just with a little bit of security addition to it, you can stave off any would-be hackers in an apartment building or in your neighborhood that could get access.

So, a good security firm will reconfigure your home routers, as well. They will install password managers, so that not only is everyone in your company able to access their passwords in a vault, but they can use really secure passwords with lots of numbers and numerals and alpha-numeric different combinations and have a secure place to store them, so if they ever need to go back because they didn't remember them, a password manager will do that for them.

A good IT firm will also install VPNs — a virtual private network — on all of your home workers and travelling workers devices, so that any transactions going back and forth, any logins, any data is encrypted through this virtual private network, a VPN, which means that any would-be hackers won't be able to get them.

The final thing that a good IT firm will do for you is it will monitor your home employees. Now listen, this is not monitoring what their activities are, but making sure they are running the moist current versions of their operating systems. You and your employees need to be running the latest version of Windows or Apple Mac IOS or your Android operating system. It is not a guarantee that you'll be secure, but trust me when I tell you, all the people that are out there that are looking to hack into a network, they are looking for older devices that they can compromise. If they see a device that is running the latest version of IOS or Windows — it's not that they couldn't hack into it, but it's not worth the time for them when there are so many other devices around the world that are running older operating systems and could be easily compromised.

A good IT firm will make sure that both you and your office and all your remote employees are running the most recent versions of their operating systems to just deter would-be hackers.

So, hire an IT firm this year. Yeah, you'll have to pay a few thousand bucks to do it, but they will make sure your people are trained. They will reconfigure everybody's routers. They will put in a password manager so people can use more complex passwords. They will install virtual private networks so all transactions are encrypted. And, finally, they will make sure everyone is running the latest versions of your operating systems.

Listen, you're not going to completely be 100% safe from any hacker, but you can minimize the risks by taking these steps, and that's what a good security firm — an IT security firm — will do for you. So, find one, ask your peers, ask your colleagues, get a good recommendation — I'm happy to give you a recommendation if you want to reach out to me, as well.

One final thing: get cybersecurity insurance, as well. Most of the main providers that are out there, they provide cyber insurance that if you do happen to get hacked or fall into that situation where you are down for a few days or, God forbid a couple of weeks, you can get some insurance to help you with it and protect you through those times.

I'm telling you, getting hacked is not a fun situation. Yet, getting back to that CNBC survey where only 5% of small-business owners are actually concerned about it compared to inflation or labor, and in my opinion, it should be among the top.

So, those are my thoughts this week. Cybersecurity not as big a concern among small businesses. You should have it as a big concern. Hire an IT firm, take the steps that I mention, make sure you are protecting your business.

Hope this information helps. You've been listening to this week's "On the Mark" episode. My name is Gene Marks. Again, if you would like to suggest any topics or guest for our podcast, please visit us at payx.me/thrivetopics . That's P-A-Y-X dot M-E/thrivetopics.

Thanks so much for listening. We will see you again next week. Take care.

This podcast is property of Paychex, Inc. 2022. All rights reserved.