Responsive Technology Partners

Issue 28 | May 2021

Coming Soon...

2020 was a year of positive change for Responsive Technology Partners and for our clients as well. With the mergers of our Roanoke, Raleigh, and Tampa offices, we are better equipped to handle any technology needs our clients may have. At the beginning of 2021, we moved to a new insurance carrier that could better support us throughout all of these markets. During the transition to our new carrier, a thorough review of all of our existing contracts was completed. As a result of this review, our new carrier has requested that we work with all of our customers to get new contracts in place that meet their requirements and provide an overall better mutual protection for us and our customers.

So, over the coming months, we will be reaching out to all of our customers to get these new contracts executed. Please feel free to reach out to your Responsive Technology Partners contact if you have any questions.

How To Build A Forward Thinking Customer Culture In Your Small Business

How well do you know your customers and clients? If you want to deliver a stellar customer experience and have a forward-thinking customer culture within your organization, you need to know your customers. What makes them tick? What do they love? Why do they make the decisions they make?

More than that, you need to go after the customers who make the most sense to your business. As you grow, you have more opportunity to be picky, so be picky! Develop the customer base you really want. That makes it easier to market to them, because you're all on the same page.

Finally, when you know who you want to target, stay consistent in your messaging. The entire customer experience – from online marketing to your storefront – should all be uniform. Consistency helps build your brand and anchors customers to the overall experience.

- Forbes, Feb. 15, 2021

How To Make Cyber Security An Ingrained Part Of Your Company Culture

Your employees are your first line of defense when it comes to protecting your business from cyberthreats. Human error is one of the single biggest culprits behind cyber-attacks. It comes down to someone falling for a phishing scam, clicking an unknown link or downloading a file without realizing that it's malicious.

Because your team is so critical to protecting your business from cyberthreats, it's just as critical to keep your team informed and on top of today's dangers. One way to do that is to weave cyber security into your existing company culture.

How Do You Do That?

For many employees, cyber security is rarely an engaging topic. In truth, it can be dry at times, especially for people outside of the cyber security industry, but it can boil down to presentation. That isn't to say you need to make cyber security "fun," but make it interesting or engaging. It should be accessible and a normal part of the workday.

Bring It Home For Your Team. One of the reasons why people are often disconnected from topics related to cyber security is simply because they don't have firsthand experience with it. This is also one reason why many small businesses don't invest in cyber security in the first place – it hasn't happened to them, so they don't think it will. Following that logic, why invest in it at all?

The thing is that it will eventually happen. It's never a question of if, but when. Cyberthreats are more common than ever. Of course, this also means it's easier to find examples you can share with your team. Many major companies have been attacked. Millions of people have had their personal data stolen. Look for examples that employees can relate to, names they are familiar with, and discuss the damage that's been done.

If possible, bring in personal examples. Maybe you or someone you know has been the victim of a cyber-attack, such as ransomware or a data breach. The closer you can bring it home to your employees, the more they can relate, which means they're listening.

Continue to page 3 to learn more.

Collaborate With Your Employees. Ask what your team needs from you in terms of cyber security. Maybe they have zero knowledge about data security and they could benefit from training. Or maybe they need access to better tools and resources. Make it a regular conversation with employees and respond to their concerns.

Part of that can include transparency with employees. If Julie in accounting received a phishing e-mail, talk about it. Bring it up in the next weekly huddle or all-company meeting. Talk about what was in the e-mail and point out its identifying features. Do this every time phishing e-mails reach your employees.

Or, maybe Jared received a mysterious e-mail and made the mistake of clicking the link within that e-mail. Talk about that with everyone, as well. It's not about calling out Jared. It's about having a conversation and not placing blame. The focus should be on educating and filling in the gaps. Keep the conversation going and make it a normal part of your company's routine. The more you talk about it and the more open you are, the more it becomes a part of the company culture.

Keep Things Positive. Coming from that last point, you want employees to feel safe in bringing their concerns to their supervisors or managers. While there are many cyberthreats that can do serious damage to your business (and this should be stressed to employees), you want to create an environment where employees are willing to ask for help and are encouraged to learn more about these issues.

Basically, employees should know they won't get into trouble if something happens. Now, if an employee is blatantly not following your company's IT rules, that's a different matter. But for the day-to-day activities, creating a positive, educational, collaborative environment is the best way to make cyber security a normal part of your company culture.

Plus, taking this approach builds trust, and when you and your team have that trust, it becomes easier to tackle issues of data and network security – and to have necessary conversations.

Need help creating a cyber security company culture that's positive? Don't hesitate to reach out to your managed services provider or IT partner! They can help you lay the foundation for educating your team and ensure that everyone is on the same page when it comes to today's constant cyberthreats.

"For the day-to-day activities, creating a positive, educational, collaborative environment is the best way to make cyber security a normal part of your company culture."

How To Know It's Time To Start Scaling Your Business

Creating a business that is scalable isn't easy, but it's necessary if you intend to grow – and grow some more. There are three simple ways to tell if you've created a business that is scalable.

You Have Positive Cash Flow Figured Out.
You've successfully built a reliable month-to-month revenue stream. It's money that you can use to invest further into your business – whether it's to pay for additional employees, technology, systems and processes or all of the above.

Everything Has Been Delegated.
Delegating is hard for many entrepreneurs. You want to have a hand in everything. But when your team keeps everything running – and everything runs even when you're not there – you're in a great place to scale up.

You Have More Control Over The People You Get To Work With.
Basically, you can start to shape your client base. If there is someone you want to say no to (say you don't have the full resources to fulfill their needs or they're just not a great fit), you can move on guilt-free.

If you have these three things in place, you have the foundation to scale up safely and to create the business you've always wanted.

- Forbes, Feb. 11, 2021

SPECIAL OFFER

Free Network Security Assessment

Fresh eyes see things that others cannot.
Our free assessment is a completely cost and risk-free way to get a credible third-party validation of the security, stability and efficiency of your IT systems.

At the end of the Assessment you'll know:

- Where you are overpaying (or getting underserved) for the services and support you are currently getting from your current IT company or team.
- Whether or not your systems and data are truly secured from hackers and ransomware, and where you are partially or totally exposed.
- If your data is actually being backed up in a manner that would allow you to recover it quickly in the event of an emergency or ransomware attack.
- Where you are unknowingly violating IRS or HIPAA regulations.
- How you could lower the overall costs of IT while improving communication, security and performance, as well as the productivity of your employees.

This assessment can be conducted 100% remote with or without your current IT company or department knowing.

Call (877) 358-9388 today to schedule your Network Security Assessment!