

# Responsive Technology Partners

Issue 48 | January 2023

## RESPONSIVE TECHNOLOGY PARTNERS ANNOUNCES ACQUISITION OF SECURIS SYSTEMS

Responsive Technology Partners, a joint venture between Pineland Telephone Cooperative, Inc. and Wilkes Communications, announced December 1, 2022 the acquisition of Securis Systems located in Tampa, Florida. Founded over 10 years ago by Mr. Jeremy Axe as a ground-up technology operation providing IT support to the food service industry, Securis Systems has gained an outstanding reputation while sharing a similar mission and core values as Responsive Technology Partners. This new location will report to Mr. José Remon, RTP's President of the Florida Market, with support from both of Responsive's operational and marketing teams.



"The addition of Securis provides a new revenue stream in the point-of-sale system implementation and management as well as a material expansion in our Florida market assisting the growing demands for cabling installation and IT services. A team of 8 seasoned IT and cabling professionals join our growing RTP family today to push our overall headcount to 77 professionals in 4 states with 10 offices in 5 years. We are truly honored to have this opportunity and look forward in continuing the outstanding growth in Florida with José, Jeremy and the hard-working Florida RTP team driving this effort." RTP's CEO Steven McComas stated, welcoming the new team.

Securis Systems founder Jeremy Axe, offering further details says, "After a decade of working and learning in Corporate IT with various Hospitality Brands, I decided to branch out and take what I had learned on the corporate side and bring it to the Tampa Bay area's local restaurant community. Through hard work and dedication to our great clients, we were able to grow from one person working out of a spare bedroom to an 8-person team serving clients throughout the United States. The growth we were able to achieve was the result of the faith our clients had in us. 95% of our growth over the years was derived from one of our existing clients introducing us to another one. That is something I've always taken great pride in."

José Remon, RTP's Florida Market President summarized the occasion by saying, "We are excited for Securis Systems to be part of RTP; our joined customers will benefit greatly with new product lines, like Hospitality, Security and Networking, as well as greater local support and availability. Both companies share the same core value system of believing that our customers come first as well as treating our employees right."

The acquisition became official December 1, 2022. To learn more about the acquired operation or its partners, visit [www.responsivetechnologypartners.com/news/](http://www.responsivetechnologypartners.com/news/)

# CYBER RESOLUTIONS FOR THE NEW YEAR

With the new year upon us, and with the energy of reflection and growth flowing, it is a perfect time to reflect on cyber security mistakes and make resolutions to follow in 2023. Every year hackers get bolder in their attacks and wiser to cyber security vulnerabilities. Here are some resolutions every employee and leader can undertake to improve cyber security for the entire business.

1

## Never Respond to Unknown Calls or Text

Every time you answer a call or text from an unknown number, you are inviting a cyber-criminal to attempt an attack. By avoiding unknown phone calls and texts, you become an increasingly difficult prospect in cyber criminal's eyes. If they can't reach you, they can't trick you.



## Keep Devices Updated

Updating your devices ensures that vulnerabilities are patched in a timely manner. Every security update to your device fixes a weakness and improves cyber security. Keep up with updates, and susceptibility to cyber-attack decreases significantly.

2

## Perfect the Password Policy

The implementation and accordance to password policies increases cyber security of the business overall. Password policies protect businesses from hackers by increasing the strength of passwords across a business. In addition, using a password manager decreases the difficulty of keeping track of complicated passwords across accounts. Password managers must be reliable and secure, so choose carefully.

3

## Multi-Factor Authentication

Multi-factor authentication builds on the already existing password policy to give an extra layer of protection against cyber threats. Using a multi-factor authentication system validates users beyond just entering a password and prevents outside users from entering the system.

4

5

## Monitor Attack Trends

Monitoring cyber-attack trends can help users predict and prevent likely cyber-attacks. Being aware of cyber-attacks that are common can help businesses to go on the offensive and stop cyber-attacks before they even begin. Monitoring trends in 2023 will prepare businesses beyond defensive actions.

## Industry Specific Risks

In addition to monitoring attack trends in general, analyzing cyber-attacks specific to your industry will push your cyber security above and beyond. The more information one has about risks against their specific business, the better equipped they are to implement protective policies. Industry specific risks require industry specific prevention.

6

# CYBER TRENDS AND PREDICTIONS FOR 2023

Threat actors are constantly evolving and changing their tactics, and cyber security efforts must evolve and change with them to ensure secure protection. In order to do this, companies must stay informed of current trends and future predictions for cyber-crime.

"The new reality is that most critical infrastructures operate in a digital environment that is internet accessible. The trends of integration of hardware and software combined with growing networked sensors are redefining the surface attack opportunities for hackers across all digital infrastructures." (Forbes).

This opens the door for cyber-attacks such as ransomware; however, not all industries will be targeted, and some are more vulnerable than others.



"Cyber criminals look for organizations or industries teetering at the edge and then make their move to tip them over. Last year, we saw that with manufacturing — a strained industry viewed as the backbone of supply chains. With the distinct possibility of a global recession on the horizon, we expect to see ransomware attacks spike in 2023. However, larger organizations in regions heavily impacted during the ransomware boom are the most prepared for this wave after investing time and money in fighting back." (Security Intelligence).

For 2023, regardless of industry, the more prepared one is for a cyber-attack, the less likely one will occur. Iron cyber defense creates less of a target for cyber criminals.

"Cyber-attackers will always look for the weakest point of entry and mitigating third-party risk is critical for cybersecurity. Supply chain cyber-attacks can be perpetrated from nation-state adversaries, espionage operators, criminals, or hacktivists. Their goals are to breach contractors, systems, companies, and suppliers via the weakest links in the chain." (Forbes).

Another cyber-attack forecasted to gain popularity amongst threat actors in 2023 is polymorphic malware.



"Polymorphic malware enabled by machine learning algorithms and eventually artificial intelligence. It could be used to bypass two-factor authentication and other authentication security measures. This type of malware is being shared more often by criminal hacking groups and could pose a genuine problem for businesses in 2023." (Forbes).

In addition to ransomware and polymorphic malware, trends for 2023 include the expansion of IoT, more bots, AI and more will all have developments beyond their current uses.



"There are many other interesting trends to look out for in 2023. These trends will include the expansion of use of a Software Bill of Materials (SBOM), the integration of more 5G networks to bring down latency of data delivery, more Deep Fakes being used for fraud, low code for citizen coding, more computing at the edge, and the development of initial stages of the implementation of quantum technologies and algorithms. When all is said and done, 2023 will face a boiling concoction of new and old cyber-threats. It will be an especially challenging year for all those involved trying to protect their data and for geopolitical stability." (Forbes).

## IMPROVE YOUR SALES TEAM AND GROW YOUR BUSINESS

It's no secret that sales can make or break any business. Without a strong sales plan and team in place, it's difficult to bring in any profit or move your products. If your business has struggled to reach its sales goals, you must reevaluate your sales process and make any necessary adjustments. Check out the following three pieces of advice to help you get started.

### ☒ Discover Your Company's Vision

Where do you want your business to be in five to 10 years? How will you get there? You need to figure this out and get your sales team to buy into your vision so they can help your business reach its goals.

### ☒ Hire The Right Team

Evaluate your current team members and see if there's anyone who is not meeting expectations. Have a discussion and try to inspire them – but if there's no improvement, find a more suitable option.

### ☒ Create A Pleasant Company Culture

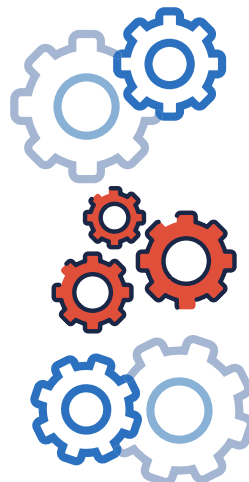
Your team members will put forth their best effort if your business is somewhere they want to work. Create a culture where everyone is recognized, is heard and has the opportunity to grow, and you'll soon notice many benefits, including sales growth.

## 2 WAYS TO REFINE WORK RELATIONSHIPS WITH YOUNG EMPLOYEES

The workforce gets younger every day, which can make things more challenging for business owners. Many have recently adapted to meet the needs of new millennial employees, but now even younger generations have started to work. This has required business owners to learn how to build meaningful relationships with these new employees. Here are a few ways you can do this, too.

### Setting Standards Early

One of the most significant concerns for business owners, especially in regard to young employees, revolves around values. It can be hard if values don't align. To avoid this situation, dive deep into this topic during the hiring process so you are well aware ahead of time.



### Giving Young Employees Responsibility

Young employees want their work to matter and their voices to be heard. Once you get them through onboarding and you're comfortable with their skills, give them a chance to prove themselves.