



An Open Letter to Our Customers

January 18, 2023

While we have always had a security portfolio at Citon, in the months since the onset of the pandemic we have witnessed an explosion in cyber-attacks and profound industry changes. In fact, after 28 years in business I can unequivocally say that these challenges and changes are the most instrumental, impactful, and significant we've ever experienced. Your business is incredibly important to us and based on the trust you have placed in Citon as your current (or future) service provider, we have made several important business and technology decisions which are relevant to you and that I want to share with you now.

As I am sure you are aware, when you read the news online or simply turn on the television, cybersecurity is a much bigger problem today than most of us would ever have imagined. Citon is receiving an unprecedented number of calls in 2023 asking for help with some form of ransomware or cyber-attack and recently released industry data backs this up... 64% of all reported cyber-attacks affect small to medium-sized businesses (SMBs) just like yours. Yet because there is such a stigma and so much embarrassment surrounding these attacks, many more of these incidents go unreported. What we do know is that these local and regional attacks are causing costly downtime, tens of thousands of dollars in recovery costs, and that more than half of the SMBs impacted by a cyber-attack fold within 6 months of the attack.

"Diagnose before we prescribe" has been key among Citon's core tenets since our humble beginnings nearly three decades ago. With this in mind, and through ongoing consultation with our engineering team, our corporate cybersecurity experts, and our industry peers, we have developed a new set of essential cybersecurity tools and services to help combat the current cybersecurity crisis. As a first step, Citon utilizes industry-leading tools and in-depth expertise to perform an individualized cybersecurity gap analysis, comparing what organizations have today, with what we know they need. Overall, our analyses show that the biggest and most common weaknesses currently center on vulnerability scanning, endpoint detection and response, network detection and response, and security awareness training.

As we face this time of unprecedented cybersecurity need together, Citon's cybersecurity services are the most important and the most comprehensive we have ever offered. This new design and evolved technology will help your organization prevent ransomware and email attacks, which the FBI highlights as the two most common forms of attack on our local and regional organizations. The value and protection these services provide has never been greater, immediately eclipsing any installation and incremental monthly costs with the benefits of an additionally advanced solution. And there's more good news: most organizations we meet already have at least a few of the required security tools in place – and typically, the most common remaining areas of critical vulnerability are rapidly and economically addressed.



In closing, although much has changed in our industry since 1994, Citon's imperative to protect and to empower our customers by securely and responsibly leveraging technology has never wavered, and it never will. We appreciate the trust you place in us, and we will never stop working to earn and to deserve that trust every day.

If you're reading this and are already a Citon customer, a member of our team will be in touch very soon to confirm the date and time for a working session where we can review the gap analysis of your current cybersecurity measures. But if you'd like to jump the queue, or if we're not currently working together, you can [contact us](#) anytime.

-Steven Dastoor, Co-Founder

p.s. Frequently I hear fellow local business owners discussing business insurance coverage for cybersecurity incidents. The **stark reality** is that many business insurance carriers and underwriters are facing a survival crisis of their own, brought on by an ongoing surge in cybersecurity losses. Even as insurance premiums skyrocket, business insurers are demanding in-depth threat assessments prior to approving or renewing coverage, imposing higher standards for preventative controls, and requiring layers of cybersecurity protection measures across their clients' organizations. Organizations which fail to meet and maintain compliance with these insurance requirements will find (sometimes too late) that their claim eligibility determination is significantly delayed, or rejected outright. We're not in the business of selling insurance here at Citon, but we are passionate about promoting cybersecurity best practices – especially when it comes to keeping your business safe. Let us help ensure that you have the knowledge, tools, and protection you need to satisfy your carrier's cybersecurity insurance requirements.