CONTACT:

Brian Suerth
Technology Assurance Group
(858) 946-2112
brian@tagnational.com

Dave Wineman, President
Abadata Computer Corp.
(989) 883-3411
dw@abadata.com

NEWS FOR IMMEDIATE RELEASE

Attackers Have Successfully Hit the Nation's Largest Corporations – Their Onslaught on SMBs Will be Worse – Are You Prepared?

Leading Managed Technology Services Provider Shares How SMBs Can Protect Themselves from Cyberattacks and Ransomware Threats

MICHIGAN – July 27, 2021 – Abadata Computer Corp., a leading managed technology services provider (MTSP), recently shared that some of the nation's largest corporations, like McDonalds, Adobe, eBay, Equifax, LinkedIn, Marriott, Target and Yahoo have all been affected by cybersecurity breaches. While many of these breaches have been widely publicized, they only represent a small fraction of the attempted cyberattacks, which the modern business owner now faces. As a result of these breaches, we are also beginning to see cybercriminals become more emboldened, targeting more critical infrastructure in an effort to demand heftier sums. In fact, recently the Colonial Pipeline, which is responsible for supplying 45% of the fuel for the East Coast, was hit with a ransomware attack. This halted gas distribution, sending customers into "panic buying" throughout the East Coast and eventually cost $4.4 million to restore. Meanwhile, JBS, one of the nation's largest meat processors who is responsible for 20% of the nation's meat supply, was also hit with a ransomware attack that they eventually paid $11 million to resolve. While most SMBs are aware of the growing threats posed by cybercriminals, they are failing to recognize that after

large corporations and major infrastructure centers fortify their cyber defenses, hackers will have no place to turn but to small business.

Abadata has been doing its best to educate business owners on the challenges that a breach, virus or phishing attack could have on any organization, and its best summarized by this statistic from the National Cyber Security Alliance, "60 percent of small and mid-sized businesses that are hacked go out of business within six months." While daunting, all this statistic actually reveals is that any preventative actions taken now, could have dramatic impacts on helping an SMB avoid these kinds of disruptions. "It's always a delicate balance," states Dave Wineman, President of Abadata Computer Corp.. "We consider it our duty to be honest in regards to the scale and scope of cyberattacks in the modern era, however, there's so much that businesses can do to protect themselves, so that they don't have to worry about these sorts of nuisances affecting them."

While an anti-virus and firewall may have been an effective security measure in the early 1990s, technology has evolved dramatically since then. There are many other technology systems available, that can fortify any SMB's defenses so that they are fully prepared and protected. Here are 6 steps that any SMB can take to protect its staff, customers and future from cybersecurity disturbances.

1. Use "Layers of Security" - Taking a layered approach to security enables damage to be quarantined, while simultaneously reducing the severity of any attack. This can easily be set up as long as the network administrator has taken good care to keep the infrastructure well-organized and properly maintained.

2. Activate Multi-Factor or "2-Step" Authentication - Most companies now require multi-factor authentication upon logging into key systems, requiring the user to confirm their identity before proceeding further, via text message or phone call. While this is likely to become ubiquitous across all platforms, especially cloud apps, other internal technology systems need to be configured to provide this basic, yet extremely effective layer of security.

3. Have a Data Backup or Data Recovery Plan - In the event of a breach or an outage, it's extremely useful to have all key data duplicated and stored securely in a remote location. Not only does this thwart less sophisticated cybercriminals who are counting on their target to be underprepared, but it eliminates the downtime that any breach or outage could cause, while employees "get things back up to speed."

4. Use a SOC (Security Operations Center) - In the same way that residential homes are supported by a remote security center, with 24/7 monitoring, notification and authority alerting capabilities, your team's devices should be similarly supported, as well. A good SOC will monitor network traffic, endpoints, logs, security events, etc., so that analysts can use this information to identify vulnerabilities and prevent breaches. When a suspicious activity is detected, your platform should create an alert, indicating further investigation is required.

5. Mandatory Cybersecurity Trainings for Employees - Unfortunately, "human error" is one of the main causes of most security breaches. If a company has not mandated cybersecurity trainings for employees, then undereducated employees can accidentally serve as a hacker's greatest ally. These employee trainings do not take very much time to complete and they can be configured to track and confirm employee progress.

6. Remove All IT Tasks from the CEO's List of Responsibilities - Not only is the CEO typically one of the people with the least amount of technical know-how in the company, but the time consumption required to build an adequate cyber defense strategy is sizable. While CEOs typically feel an obligation to keep their team protected, CEOs should be spending the majority of their time thinking strategically and focusing on how to create more opportunities for revenue growth, not tinkering with IT tools that they don't have full mastery over. At this stage, consider consulting with or hiring an expert IT advisor to guide you through the nitty-gritty of installations, monitoring and ongoing management of critical security systems.

While hackers continue to search for targets, the steps outlined above are immediately actionable and will serve as a solid foundation for the majority of businesses that wish to prepare themselves for the coming trend.

ABOUT ABADATA COMPUTER CORP.

Abadata Computer Corporation was started in 1981 by David W. Wineman as the Michigan Distributor of US Robotics modems and equipment. Shortly thereafter, ABADATA started the network integration segment of the business by selling, servicing and installing network equipment. Abadata has placed the utmost importance on the technical expertise

of its staff, and each employee possesses multiple certifications in various network and telephony-based systems. Abadata has been serving the needs of nearly every industry for over 35 years and has deployed technology solutions in industries ranging from education to medical to government to much more.

Abadata's mission is to make computerization magically easy. This idea is best personified by the "Magic the Bunny" who can be found on the company logo. Whether Abadata is serving its customers with antivirus, education, web, customer service or telephony needs, and customers can rest assured that Magic will be present. Abadata is committed to providing these kinds of experiences for their customers.

In addition to ease of use, Abadata has also been committed to utilizing technology to increase their customers' profitability and provide them with a competitive advantage. By concerning themselves with their customers' bottom line, they've have aligned themselves with their customers' goals and as a result they've established strong relationships across the board.

The company philosophy is to continually be on the leading edge of technology. David Wineman, CEO, states, "forward-thinking companies take on significantly more risk for the benefit of their customers. Throughout the years, we've learned that our customers appreciate our proactive approach to solving problems.

Abadata has consistently been at the forefront of advancing technology for Communication Systems, cloud and online storage, back up services and Computer Technology. In Abadata 2012 successfully purchased another Michigan company, Chris Consulting. Today Abadata has 12 professional employees and continues to uphold the same values that they started with in 1981. They understand that education and integrity are vital to creating lasting customer relationships, and the company consistently works at making sure these characteristics are at the very core of Abadata.

In 2011, in the pursuit of knowledge and better resources, the company became a member of Technology Assurance Group (TAG), an international organization representing nearly $350 million in products and services that provides the competitive advantages necessary to propel unified communications companies to regional dominance. For more on Abadata please visit www.abadata.com or call us at 989 883 3411.

###