

ACE Technology Group

March of 2022 celebrated the 20-year inception of ACE Technology Group. The year was 2002, the “Dot Com Bubble” had just burst, and owner and CEO, Chris Shank, had been laid off just days before his wife was due to deliver their first child. What better time to start a business in a new market with an unproven business model than directly after a global technology industry crash?

Two decades ago, small business computer support was on a break-fix basis; usually with a pre-paid block of hours that you could use as needed or on a schedule. A technician would come by your office on specific days, maybe a few times a month, to perform routine maintenance, verify backups were completing, and help employees with any outstanding issues. This model was a win for the IT company but not for the client. The IT company got paid before any work was performed and had little incentive to perform preventative maintenance. If the client had a computer problem, they would typically have to wait for the pre-scheduled day or pay for an emergency visit. This reactive model proved very inefficient for small businesses, and having worked at several large companies, Chris saw the added productivity value of having IT professionals proactively manage the network of computers while also being available to employees for immediate support. So began his mission to find a solution for companies

of all sizes to have secure, affordable, and reliable technology to keep their businesses moving forward.

Putting the Internet to work, Chris understood that remotely supporting IT infrastructure would be an efficient way to “transport” a tech instantly to any office. Remotely supporting employees and businesses without travel time would give companies an affordable option for on-demand IT support without the costly overhead of having their own in-house IT department. Chris envisioned this “Remote IT Department” as a model that would make ACE different, faster, and better than the traditional break-fix consultancy operations that were available at the time. He did not want his new company, aptly named ACE Technology Group, to be categorized as another “break-fix” shop or typical IT consultancy. These archaic business models required customers to have problems so they could “fix ‘em and bill ‘em”. Using the novel concept of remote monitoring and support, coupled with his software engineering background, Chris was able to automate proactive maintenance and develop a fixed-fee business model allowing ACE to align its goals with our clients’ goals — trouble-free IT at an affordable price without the unexpected costs that come from poorly maintained systems.

In 2002, the remote IT management industry was in its infancy and wildly uncertain. ACE was at the forefront of the technology offerings as Chris worked to



CHRIS AND ANDREA SHANK

assemble a toolkit for his fledgling company including remote access tools, ticket tracking, network monitoring, and billing. After a few years, the industry began to mature, and we had professional-grade tools at our fingertips. Our industry was finally given a name, Managed Service Providers or MSPs. But even back then, ACE was ahead of many of its peers. Chris envisioned ACE not only to be a “Remote IT Department,” but also wanted to include an “Enterprise-Grade IT Infrastructure” that we could extend to our clients. We offered centralized hosted email (with spam & virus cleaning) when many other IT shops were still struggling to support on-premises email servers. ACE also offered remote offsite backup directly to hard disks as part of our standard service plan at a time

when most of our peers were still backing up each customer to a local tape drive; a cumbersome process, prone to failures, slow restores, and a requirement for human intervention to rotate the tapes.

Twenty years later, ACE Technology Group continues to innovate and provide enterprise-grade IT services and infrastructure to help small businesses become more productive, agile, and secure. ACE has a full Infrastructure-as-a-Service (IaaS) hosted cloud offering that reduces costs for our clients by eliminating the large capital expenses associated with owning a physical on-premises server.

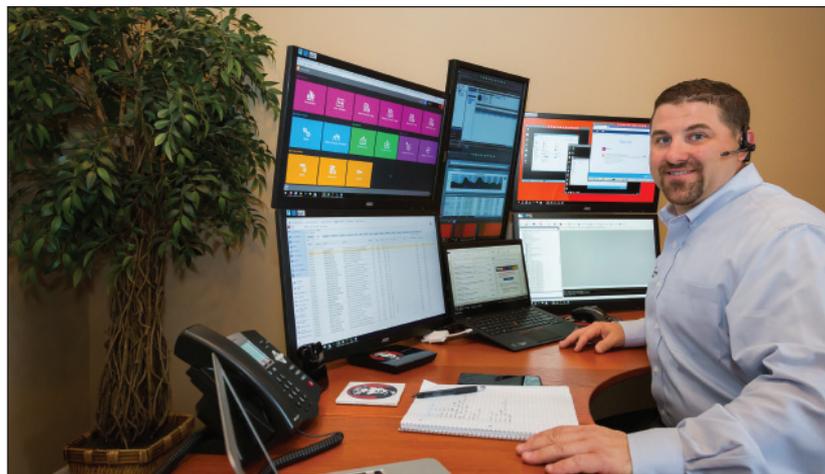
Our attention to security also sets ACE apart from our peers as we integrated modern cybersecurity tools and services into the fabric of our service and corporate culture as standard practice





almost a decade ago. Today, it's not a matter of if your company will face a cyberattack, it's a matter of when. Cyberattacks target large and small businesses alike and can leave irreparable damage. It's critical for companies to properly secure their technology infrastructure in order to protect their businesses and customer data. Cyber threats and scams are always changing and evolving, requiring businesses to constantly adapt to the world around them. Armed with this knowledge, ACE not only examines everything we do through a Cybersecurity lens, we also proactively look for vulnerabilities in our clients' environments so we can advise and assist them to develop a strong Cybersecurity posture.

We believe the job of an IT service provider is to protect the company from one of the largest, yet often overlooked contributors to cyberattacks — untrained employees. Gone are the days of employees getting away with saying "I don't know computers" and abdicating any responsibility for what happens to your network from their computer use. Employees must be responsible computer users, but employers must, in turn, provide proper computer and cybersecurity training. Just as you wouldn't allow



an untrained person to operate a forklift or delivery truck, you shouldn't let an untrained employee operate your business computer. After all, that computer may be a gateway to your financial data, the applications that operate your business, and your customers' personal data; any of which could be compromised or destroyed in a cyberattack.

Businesses can help their employees become responsible technology users by employing security methods composed of multiple layers of mitigation. Anti-spam & virus filtering systems should be integrated into all corporate email; this is

your first line of defense. Anti-virus software (AV) should be installed on every computer and maintained daily with updates. A "Next Generation" firewall with active security and threat detection is needed to guard against modern Internet threats. In addition to these layers, we offer services to test and train your employees by emulating phishing scams, as well as micro-quiz trainings and overall employee security scoring for your organization. Ongoing cybersecurity testing and training help your employees to recognize attacks and stop them dead in

their tracks before they cost your business untold amounts in damages.

Finally, it's imperative for every business to have a functioning and dependable Backup and Disaster Recovery (BDR) plan in place to recover company data quickly and thoroughly. A BDR plan is key to ensuring that businesses can quickly recover from minor incidents, such as accidentally deleting a file, or catastrophic events, such as a flood, fire, or a ransomware attack. An off-site backup allows businesses to fully restore lost data or quickly create a cloud instance if a physical server is lost or compromised. These are key features that businesses should have in place to protect their livelihoods and employees from the ever-growing threat of a cyberattack. Because ACE has already integrated these security and recovery capabilities into our service offering, our clients get all the benefits of our enterprise-grade technology platform without the high capital expense and maintenance costs.



If you'd like to get to know ACE Technology Group or get a free cyber security audit, please visit us at <https://www.acetechgroup.com/cybersecurity-report/> or call 610.640.4223 and ask for Chris!