DRaaS for Azure

11:11 SYSTEMS

Crest Furniture Overcomes Ransomware, Bolsters Disaster Recovery Strategy with 11:11 Systems

crest furniture inc.

Challenges:

- Managing rapid data growth and retail location expansion
- Navigating ransomware attack amidst cloud migration and DR implementation
- Rebuilding servers and systems while maintaining business continuity
- Lacking a fully implemented DRaaS solution at the time of ransomware attack
- Finding the right balance between in-house team skills and partner support

Solution:

- 11:11 DRaaS for Azure

Benefits:

- Achieved full data recovery within 10 days of attack without paying ransom
- Secured vital business operations and completed Azure cloud migration
- Leveraged tested 11:11 DRaaS capabilities for faster recovery times
- Gained peace of mind by ensuring future resilience to IT disasters
- Built a trusted partnership with seamless, ongoing support

Profile:

- Industry: Furniture Retail
- Size: Commercial

Client Profile

Crest Furniture, Inc. is a privately held retail furniture company headquartered in Dayton, New Jersey. Founded in 1971 by Simon Kaplan—a World War II veteran and purple heart recipient—Crest has grown from a single store into a family of companies that includes both Value City NJ Furniture and Ashley HomeStore. Today, it operates 20 retail locations as well as a 234,000-square-foot, state-of-the-art distribution center that sources and ships products from name brands like Ashley, Signature Design by Ashley, Benchcraft, Coaster, Sealy, Stearns and Foster, and Tempur-Pedic. Crest boasts everything you need to make your home look beautiful. For more information, please visit crest-furniture.com.

"Trial By Ransomware"

The story of William Stochel's introduction to life at Crest Furniture is not for the faint of heart, especially for those who work in IT. To hear him tell it—as you soon will —those first few months on the job were something of a "trial by fire."

Prior to Mr. Stochel's arrival as IT operations manager, the family-owned, New Jersey-based furniture company had begun a rather extensive IT modernization effort. With the business and its data growing at a rapid pace, the plan was to migrate much of the company's on-premises infrastructure to the Azure cloud. In order to fully unlock the scalability, performance, and reliability of the cloud, the company also wanted to ensure its data and applications would be secure and easily recoverable once migrated.

The only problem was those workloads, well, they never arrived. Not completely, at least. Not according to plan. The wrench? "We were hit with ransomware," said Mr. Stochel, delivering perhaps the most dreadful sentence in all of IT.

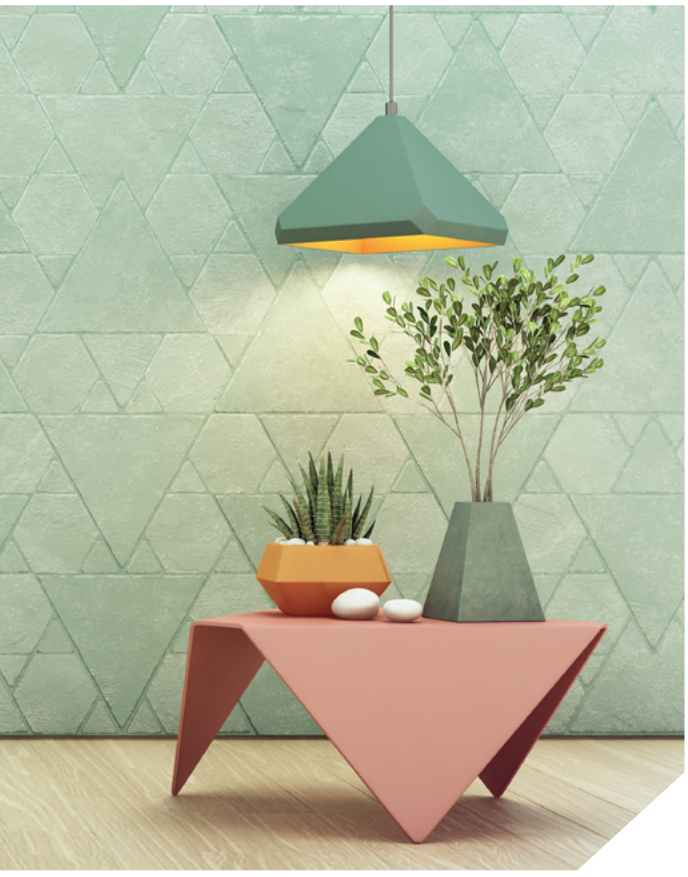
At this point, Mr. Stochel was mere weeks into his role at Crest, still learning the ins and outs of the company and its systems. To complicate matters, Crest's cloud migration as well as its partnership with 11:11 Systems for Disaster Recovery as a Service (DRaaS) remained a work in progress. This left the company open to risk and unfortunately, as Mr. Stochel says, "hackers will be hackers."

True to form, the attack occurred on a Friday afternoon before a long weekend. All of sudden, Mr. Stochel was on the clock with upwards of 15 people packed into his office, trying to figure out what went wrong. An IT veteran of nearly four decades, Mr. Stochel was recruited to help Crest through its digital transformation journey. He would need every second of that experience to help the company through just that day, let alone the rest of its cloud migration.

"This wasn't my first ransomware attack, unfortunately. I've been in the industry for a long time and have seen my fair share of high-pressure IT situations," said Mr. Stochel. "It's never a good feeling when you have to deal with an attack like this, especially in my position. At first, you're just thinking, 'What happened? Why are we down?' and then you realize what's really going on and there's just an immediate, knee jerk reaction that kicks in. 'Oh no. Let's get on the phone and start figuring out how to fix it.'"

Ultimately, time—and a little bit of luck—was on Mr. Stochel's side. While Crest's migration into the Azure cloud wasn't complete, it was complete enough. Backups allowed the company to resume business within a day, and, thanks to the tireless work of Mr. Stochel and his team, Crest fully and completely recovered from the attack in about 10 days.

"I had been on the job for only a month and a half at that point. It was a weird, intense way to get introduced to every single component in the company. It was a real crash course that I wouldn't necessarily recommend. But somebody was definitely watching over me. The timing turned out to be impeccable," said Mr. Stochel. "Basically, we were three weeks into the migration when we got hit. We had most of the key servers—including the shared drives and folders with everyone's files—already up in the Azure cloud. So, we decided not to pay the ransom and rebuild the rest of the servers internally. We just went live. It was a trial by fire, as they say. Or, rather, a trial by ransomware."



"I've been working in IT for 38 years now. I've seen and done a lot, dating back to the very beginnings of virtualization. I've built thousands upon thousands of virtual servers and worked with countless IT partners and service providers. At the end of the day, it always comes down to the people behind the technology. That's why I appreciate 11:11 Systems so much. We've built up such a good rapport. I know their team by name. When I call, I know exactly who's going to pick up."

William Stochel, IT Operations Manager at Crest Furniture

Cybercrime: No Longer if, But When

Ultimately, Crest emerged from its brush with ransomware relatively unscathed. In that regard, the company is a success story. It's also a cautionary tale.

Who knows where Crest would be had the attack occurred earlier in the company's migration journey; if Mr. Stochel and his team did not have clean, up-to-date backups on hand; or if they did not possess the skills or resources to rebuild the necessary servers in-house. The situation, Mr. Stochel says, could have turned out much, much worse.

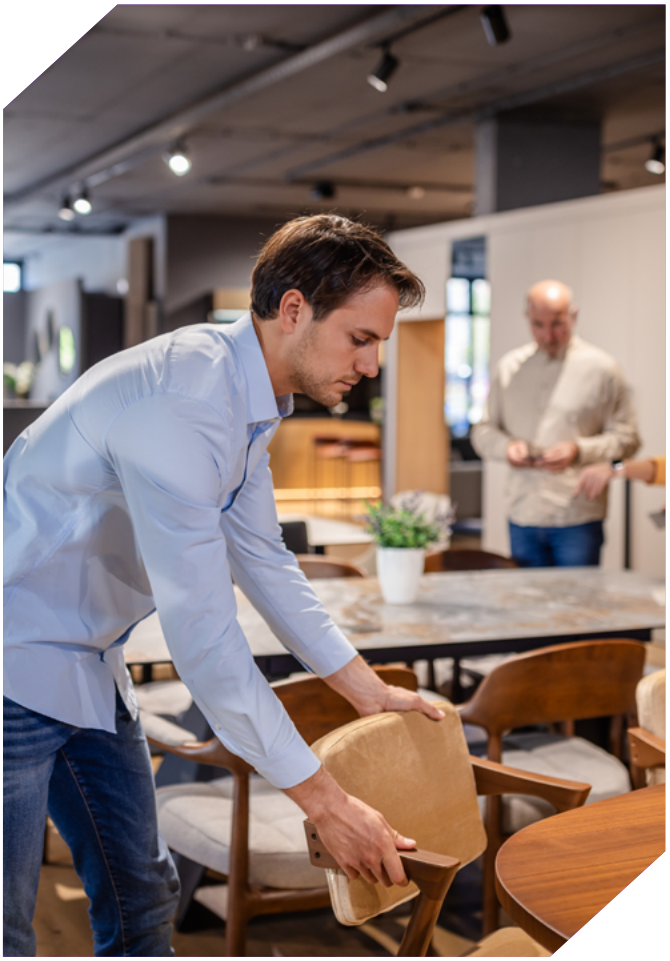
"It's definitely a good lesson to go through. It's a hard lesson. If we didn't have those servers, it could have been an expensive lesson, too," said Mr. Stochel. "The attack could have been worse, for sure. We could have lost everything, but luckily we did not."

In today's modern IT landscape, ransomware is firmly entrenched as the No. 1 cyber concern among business and IT leaders. It is both the most common and most impactful cause of IT outages, extracting hundreds of millions of dollars in damages each year.

According to research by Cybersecurity Ventures, a ransomware attack occurs roughly every 11 seconds. By 2031, they expect that gap to close to every two seconds. As a result, the overwhelming majority of experts and security analysts have begun to acknowledge an unfortunate truth: It is no longer a matter of if you will be attacked, but when.

For exactly this reason, Crest prioritized finding a DRaaS partner at the onset of its cloud journey. After a thorough market evaluation, they turned to 11:11 Systems for 11:11 DRaaS for Azure, which provides fully managed, validated recovery in the Azure cloud. And while Crest was attacked before that solution could be fully spun up, 11:11 was still able to help—by adhering to a standard migration process that requires a complete backup before moving any data.

Now that the worst is over and Crest has fully migrated to the Azure cloud with 11:11 DRaaS for Azure, Mr. Stochel knows the company is better prepared for the next disaster, whether they're facing down mother nature, human nature, or faceless threat actors. Additionally, he believes their ability to respond and recover would have been even easier had the migration been complete before the attack.



"At the time of the attack, we obviously weren't finished with 11:11 DRaaS project. But now everything is up and running and we're able to get a working copy of our DR site in minutes. We've tested it. Going forward, it's going to provide tremendous value," said Mr. Stochel.

He continued: "If we were able to failover with 11:11 DRaaS for Azure in the aftermath of the attack, it would have been amazing. Based on our testing, I think we could've been fully back up in 15 minutes, as opposed 10 days. For someone in my position, that's such a great feeling to have. I can sleep better at night knowing, if it does ever happen again, we have a DR solution in place that we've tested and we can count on to recovery quickly."

True Recovery with 11:11: The Right Technology, People, and Processes

When facing an IT crisis, time is of the essence and attention at a premium. There simply isn't enough of either to go around, as Mr. Stochel can attest. Success in these tense moments, when the alarms are sounding and adrenaline is pumping, requires more than just the right technology.

11:11 believes that true recovery combines the right technology with the right people and a trusted, tested set of plans and processes. Putting in the preparation required to achieve true recovery allows IT professionals like Mr. Stochel to confidently and seamlessly keep their organizations up and running before, during, and after potentially devastating disaster events. No matter what.

"I've been working in IT for 38 years now. I've seen and done a lot, dating back to the very beginnings of virtualization. I've built thousands upon thousands of virtual servers and worked with countless IT partners and service providers. At the end of the day, it always comes down to the people behind the technology," said Mr. Stochel. "That's why I appreciate 11:11 Systems so much. We've built up such a good rapport. I know their team by name. When I call, I know exactly who's going to pick up."

Backed by the award-winning technology and world-class people at 11:11, which completely manage Crest's DR needs from end-to-end, Mr. Stochel and his team can focus on delivering business value instead of worrying about recovery. In the event of a disaster or unplanned downtime scenario, 11:11 will not only be able to failover the company's virtual machines (VMs) to the desired Azure cloud region, but will also validate recovery and debug VMs, if needed.

"From beginning to end, the 11:11 team has been great," said Mr. Stochel. "They moved quickly and efficiently through the design and implementation process and our testing requirements. They were also very thorough, putting a ton extra effort into every conversation and providing all the documentation we could need—and more."

> "When disaster strikes, and it doesn't even have to be as serious as ransomware, the pressure on IT ramps up. Just because you're having a problem doesn't mean that everything else has stopped, right? And once that snowball gets rolling, it's hard to stop. So, to know that I'm able to shoot 11:11 an email and say: 'Hey, I'm having this problem. Can you check it out while I take care of these other six fires and meet back in 15 minutes?' That's enormously valuable. Those are the relationships that I've come to appreciate the most over the years."
>
> William Stochel, IT Operations Manager at Crest Furniture