Makaye InfoSec

Your Dedicated Cybersecurity Team

THE JAMES L. WEST CENTER FOR DEMENTIA CARE CASE STUDY

Nursing an ailing cybersecurity program back to good health.

Makaye InfoSec
Your Dedicated Cybersecurity Team

CASE STUDY
2020

1 Problem

After cybercriminals attacked the James L. West Center for Dementia Care with ransomware, the Center realized how vulnerable they were – and how at risk of losing their cybersecurity insurance.

2 Solution

Makaye Infosec was able to develop a comprehensive, tailored infosec program – from initial assessment to full implementation – through easy, palatable steps.

3 Benefits

- Better security: Continuously improving security scores
- Peace of mind: Knowing they have the power to prevent and address future threats
- Renewed insurance: With a plan in place to stay secure, their insurer was happy to renew

OVERVIEW

The James L. West Center for Dementia Care (JLWC) is a not-for-profit organization that provides specialized care to a vulnerable population. The faith-inspired, community is dedicated to personalized and compassionate care of people living with dementia, Alzheimer's, and similar disorders. They also offer specialized education for caregivers, healthcare professionals, and the community at large.

CHALLENGE

The quality of care they can provide relies on the smooth day-to-day operation of their IT infrastructure and equipment, so when they were attacked with ransomware – an all-too-common form of cyber-attack where criminals shut down IT systems until the victim pays up – it was a wake-up call that their cybersecurity protections needed strengthening.

Thankfully, no patient data was breached, but the experience made clear that their security protocols needed a booster. If nothing else, their insurance provider demanded it: "Fortunately, we had cybersecurity insurance," says Center President and CEO Cheryl Harding, "but they would not have renewed our policy if we hadn't put a good cybersecurity plan in place."

JLWC turned to Makaye Infosec for help. “Other providers couldn’t articulate what they would do to make sure we were secure,” Harding says. “Makaye Infosec very clearly spelled out what our security goals were and how we would get there.

As a healthcare organization committed to the wellbeing of its patients and their loved ones, JLWC both provides critical services and hosts sensitive data, and the organization takes its legal and ethical obligations very seriously.

They also have ambitious plans for future growth that could be undermined or even derailed by a security threat down the road. After the ransomware incident, they didn’t want to take any chances. However, they didn’t know where to start. “We didn’t even know how vulnerable we were,” Harding says.

SOLUTION

For that reason, Makaye Infosec began with a routine check-up: a thorough security assessment leading to a detailed roadmap to chart a path from JLWC’s initial security posture to their final organizational goals. That meant balancing twin priorities: covering infosec requirements from every conceivable angle while breaking the roadmap down into practical, realistically achievable action steps that fit within the organization’s available resources and budget.

It helped that Makaye Infosec focuses exclusively on cybersecurity but could work collaboratively with their IT provider. With each group dedicated to their own specialty, they could collectively provide the best-of-all-worlds: strong security and efficient IT, without compromising either group’s priorities. Thus, Makaye was able to provide security oversight without stepping on anyone’s toes.

“Having the Chief Information Security Officer from Makaye InfoSec reporting to me, separate from the IT person, is very similar to something we do in healthcare,” Harding explains. “That’s when we have a risk manager that typically reports directly to the CEO or administrator rather than the nurses, because they’re holding that nurse accountable, so it’s very similar to what we do internally.”

Simultaneous with implementing the new security plan, Makaye Infosec was also able to help educate JLWC personnel – communicating what threats they were facing and how to mitigate them – while translating technical cyber security needs into plain language and connecting the dots with larger business objectives. Ultimately, cybersecurity is a function of business strategy, not an add-on. The result has been a healthier security posture that continues to improve over time. “I believe that our relationship with Makaye Infosec will be very long-term,” affirms Harding.

RESULTS

Improved Security

"We've improved our security scores and are more secure, and I love seeing those charts and measures show it."

Cyber Policy Renewed

They were impressed that we already had a plan in place to stay secure. They were happy to renew at that point."

Peace of Mind

"It gives me comfort knowing that the IT group has oversight from the Infosec group. I wouldn't do it any other way."

Happier Staff

"A lot of our staff are satisfied with [the service]. They are complimentary about it and pleased."

"The biggest benefit to me is that I now know, while we're not bulletproof, we have a way to address it if something happens."

Cheryl Harding,
President and CEO
of the James L. West Center
for Dementia Care

Your Trusted Cybersecurity Partner

If you need help addressing your cybersecurity concerns, Makaye Infosec has extensive knowledge and expertise in securing and protecting healthcare providers.

Contact us today for a free consultation and find out how a Cybersecurity Maturity Assessment can help you secure your organization and achieve HIPAA compliance.

Makaye InfoSec

Your Dedicated Cybersecurity Team

George Makaye, CISSP
smla@minfosec.com
(972) 645-2218
www.minfosec.com