Fortified
HEALTH SECURITY

CASE STUDY

How a Hospital Solved their Cybersecurity Staffing Challenges

The challenges of cyber tech and labor market competition

The pandemic exacerbated the cybersecurity challenges of a non-profit community hospital, which included:

- Staffing
- Maintaining skill sets and certifications
- Budget limitations

Fierce competition in the labor market compounded these challenges, making it difficult to find qualified cybersecurity experts. To address their most pressing needs, the hospital's Chief Information Officer (CIO) looked to a few outside consulting groups.

"Despite having some positive initiatives in place, the combination of the pandemic and the ever-changing threat landscape meant that we weren't making the progress we needed to," explains the CIO. "We brought in a few vendors on short-term contracts, but projects would kick off and then lose momentum. Their focus was also limited to short-term maintenance, leaving us without a long-term visionary strategy or a clear roadmap to reach our goals."

Health System:
Non-profit community hospital serving adults and pediatric patients

Location:
Western United States

Number of Beds:
250 - 350

The importance of healthcare expertise

It quickly became clear just how essential it was to find a cybersecurity partner who understood healthcare.

"When you account for the human dynamics within a hospital environment, the competing priorities of the doctors, nurses, patients, operational staff, and the financial pressures, having technical cybersecurity know-how isn't enough," says the CIO. "For cybersecurity to be effective in a healthcare setting, you must understand the nuances that make healthcare cybersecurity more complex than other industries. It's about striking that delicate balance between protecting information and not disrupting patient care."

After struggling to effectively tackle their immediate issues and long-term objectives, the hospital realized that they needed an experienced healthcare cybersecurity partner that could be an integral part of their team.

> **"It's about striking that delicate balance between protecting information and providing quality care."**

A tailored solution

To find the right partner, the CIO reached out to his network of security and cybersecurity professionals. A few people pointed him to Fortified Health Security, telling him, "This is the group you need to talk to."

It was clear from the start that Fortified understood the level of responsibility and concerns of the CIO, what cybersecurity means in a hospital environment, and what needs to be done every day to protect the hospital.

After learning more about the hospital and the needs of the CIO and his team, Fortified recommended starting with their Virtual Information Security Program (VISP) and Risk Assessment service.

As part of Fortified's VISP, the hospital would have a dedicated Information Security Analyst and a virtual information security officer (VISO), a highly experienced healthcare cybersecurity leader, to guide and oversee the implementation of their cybersecurity roadmap.

"The fact that Fortified's Virtual Information Security Program includes a VISO and an infosec analyst really sets them apart. Right out of the gate, I felt that I had a partner who would address our most pressing needs while also helping us build and implement our long-term plan over the next several years," says the CIO.

The implementation journey: Building a risk profile

To get a baseline for what people, processes, and technology were in place at the hospital, Fortified's risk assessment team used the NIST Cybersecurity Framework to conduct and map a HIPAA risk assessment.

The risk assessment gave the CIO a clearer picture of where to focus and prioritize. It also illuminated all the disparate tools they had in place that were adding significant cost and time, but not value.

Armed with a better understanding of their present cybersecurity state and maturity path, the CIO and his VISO worked together to present their findings and recommendations to the executive team.

"Our VISO took the time to truly understand my perspectives and the unique dynamics of our hospital to build a customized plan for our hospital," shares the CIO. "They also worked tirelessly to help me present that story in a clear, compelling, and condensed way, which was crucial to helping me get buy-in from our executive team and board."

In addition to providing both tactical cybersecurity support and strategic guidance, an essential role the VISO plays is building relationships and bridging gaps between departments to strengthen the overall cybersecurity posture of the organization.

"How people think, feel, and behave is deeply connected to cybersecurity's success or failure. This is why having someone who understands the human elements of cybersecurity and how to build relationships with people is so vital. Our Fortified VISO gets that," says the CIO. "They didn't just come in, do a risk assessment, and treat our hospital like any other hospital. Instead, they listened to and partnered with our other IT and compliance leaders throughout the organization. They took the time to genuinely build relationships, understand all the dynamic variables at play, and gain that institutional knowledge."

> “
>
> **Right out of the gate, I felt that I had a partner who would address our most pressing needs while also helping us build and implement our long-term plan over the next several years."**

With a robust cybersecurity roadmap in place, and stronger partnerships developed across departments, the CIO and his VISO moved forward with implementing other essential cybersecurity services through Fortified, including Security Information and Event Management (SIEM), Vulnerability Threat Management (VTM), Security awareness training, Penetration testing, and Managed Detection and Response (MDR).

Transformative results: Creating a more efficient cybersecurity program

By consolidating their services with Fortified, the hospital has been able to:

- Reduce their vendor threat risk
- Develop a more efficient cybersecurity program
- Ensure continuity and reliability
- Diversify and reallocate spend

Fortified Central Command has also been a game-changer for the CIO and the security team.

"Central Command truly set us up for long-term success. The fact that I can log into one dashboard and see our Fortified services in one place has been transformative in terms of visibility, collaboration, time savings, monitoring, and reporting," says the CIO. "My team and I no longer have to log into five different platforms to get the information we need, which helps us simplify how we manage our cybersecurity program."

The CIO and his security team have transitioned from relying on short-term fixes to adopting a more reliable and consistent cybersecurity strategy. This shift has enabled them to make continuous progress while effectively managing costs.

"Partnering with Fortified and our incredible VISO has given me peace of mind. We're not only doing the right things to protect our hospital and our patients, but we're also building confidence and trust in the process, which is vital," says the CIO. "The strides we've made since joining forces with Fortified have been nothing short of revolutionary, and I can't express enough how much of a positive impact they've had within our organization."

www.fortifiedhealthsecurity.com
connect@fortifiedhealthsecurity.com
615.600.4002