

How a Community Health System Reduced their Cybersecurity Vulnerabilities



Barriers to an efficient cybersecurity program

For a leading community health system, the greatest barriers to managing their cybersecurity program efficiently and effectively included:

- Inconsistent cybersecurity leadership
- Complex staffing challenges for multiple cybersecurity roles
- Staying compliant with privacy regulations and security standards

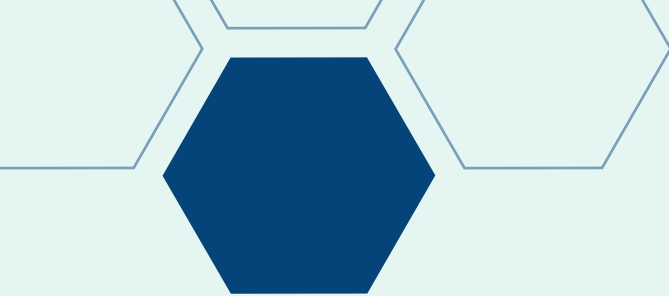
“At the time, the team was small and had minimal cybersecurity experience. They were doing basic day-to-day information security, but there was no vulnerability management or even a strategic plan for how we were going to build and manage a true cyber program,” explains the health system’s current Information Security Officer (ISO).

The health system’s leadership attempted to hire full-time employees for these roles, but quickly discovered how difficult and time-consuming it was to do so.

Client Profile: A leading community health system providing care to underserved and vulnerable populations.

“People in cybersecurity are in high demand, so your hiring process needs to move quickly, and compensation needs to align with the competitive landscape. Our hiring process takes longer than other organizations and it’s challenging to match their pay expectations,” shares their ISO. “Another major obstacle was finding people with cybersecurity expertise, and healthcare knowledge and experience. That combination is incredibly rare.”

As the health system’s human resources and cyber knowledge gaps increased, they struggled to meet minimum security and regulatory standards. The organization also lacked security policies and procedures, and a framework that allowed them to show their cyber maturity over time.



Scaling solutions and skills

“The health system started contracting with Fortified Health Security to address some of their most pressing cybersecurity needs, including:

- Penetration testing
- HIPAA-focused risk assessments
- Vulnerability and threat management
- Managed phishing
- Third-party risk management (TPRM)
- Managed 24/7 security monitoring through Fortified’s Security Information and Event Management (SIEM) program
- Cybersecurity guidance and leadership expertise with a Fortified Virtual Information Security Officers (vCISO)

“The cybersecurity services Fortified provided us were invaluable. They brought visibility into our most acute vulnerabilities as well as a roadmap to remediate them, which took a lot of pressure off the team. However, we realized that we still didn’t have the capabilities to manage and address these vulnerabilities,” says their ISO. “For example, Fortified would provide us with vulnerability reports, but it was up to us to digest those reports, disseminate that information, put together a strategy and plan around remediation, and execute on

it. While all these insights were useful, our team simply didn’t have the expertise or bandwidth to do that.”

To determine how to fill these additional human resources gaps, the ISO sought the expertise of their Fortified team.

“We knew from years of experience that hiring full-time employees to do this type of work would be incredibly difficult, from both a budget and a proficiency standpoint. Because we had such a positive and productive partnership with Fortified over the years, we decided to expand our contract with them to leverage their Expertise On Demand (EOD) services,” explains their ISO.

Through the EOD program, Fortified provided the health system with three full-time team members—one team lead and two security analysts— as dedicated support to the organization.

Executing on-demand expertise

Prior to bringing on EOD team members, the health system was leveraging the expertise of a virtual information security officer (vCISO) through Fortified’s Virtual Information Security Program.

One of the first responsibilities that the vCISO took on was building policies and procedures to help the health system align its entire IT team with the NIST cybersecurity framework (NIST CSF).



HIPAA is great, but we knew we needed to establish a framework that reflected our guidelines, best practices, and standards, and tracked our cybersecurity progress and maturity over time. Our vCISO was instrumental in helping us develop our NIST CSF pillars, and prioritize what we needed to focus on at each phase of our roadmap.

With the NIST framework developed, the health system was able to focus their three full-time EOD team members on carrying out the tactical elements of their cybersecurity priority list.

“Developing our NIST framework with our vCISO was a big step. But doing the actual work to execute on that framework is an ongoing and evolving process. Our EOD team started by focusing on our large, risk-oriented programs, and helping our vCISO develop our policies and procedures—from our firewalls to our e-mail delivery solution and everything in between,” says their ISO. “From there, they began looking at our cybertechnology tool stack, what’s being managed and what’s not, where we’re lacking, and what we need to be doing. Now, the team is getting into the groove of ongoing monitoring and assessment, and reporting on corrective actions that they’ve uncovered and remediated.”

Central Command, the unified platform Fortified Health Security uses to deliver services to clients, has also been essential to the health system’s ability to implement their cybersecurity services efficiently and effectively.

“Fortified Central Command has transformed how we manage our cybersecurity program. Before having this type of unified platform, I’d have to go to a half dozen or more tools to pull data, aggregate it, create reports, and send multiple versions out to different stakeholders. That consumed a lot of time,” explains their ISO. “Now, my team and I simply go to Fortified’s Central Command platform, and it consolidates all the essential information we need from all our various security tools. It’s a massive time-saver and has significantly improved our efficiency. Plus, the mobile app capability means my team doesn’t have to be sitting in front of their computer to see alerts from our SOC team and react immediately.”

Increasing cybersecurity confidence

Since partnering with Fortified Health Security in 2019, the health system has been able to:

- Address their cybersecurity leadership needs
- Fill their staffing gaps
- Develop a NIST cybersecurity framework
- Improve and track their cybersecurity maturity over time

They've also been able to effectively convey how the services, systems, tools, people, and frameworks they've advocated for over the years have helped improve the security posture of their organization.

Specifically, they've seen:

- Their NIST CSF scores increase by nearly 30%
- Critical, exploitable vulnerabilities reduced by nearly 20%
- High, exploitable vulnerabilities decreased by nearly 32%

"Being able to show our progress to our leadership team and board, and explain exactly how we're driving our cyber program forward, has been invaluable," says the ISO. "Before partnering with Fortified, we didn't have the visibility into where our vulnerabilities were because we didn't have the staff to run those scans. Now that we do, I sleep a lot better at night."

Working with a partner who acutely understands the intricacies of healthcare and how that impacts cybersecurity has also been pivotal to the health system.

"There are many cybersecurity providers that understand the technical aspects of what needs to be done and why. But if they haven't applied that knowledge within a healthcare organization, they just don't get it. And that makes it difficult to make real progress," says the ISO. "With Fortified, I don't have to sit there and explain repeatedly why I can't do something or why we can't patch a certain vulnerability related to a medical device. They already know the answer. In fact, many times they guide me on what we should do so that we don't inadvertently break something critical to serving patients. Having a partner with that experience and expertise is priceless."