CUSTOMER CASE STUDY

Strengthening Cybersecurity Posture:
Saint Michael's College Partners with Towerwall

towerwall

2025

OVERVIEW

Saint Michael's College is a private Catholic liberal arts college in Colchester, Vermont, founded in 1904 with a student body of 1,200 and nearly 400 staff.

BACKGROUND

Joe Pawlaczyk, Chief Information Officer (CIO), having limited resources and budget, sought to mature the institution's cybersecurity capabilities and turned to Towerwall. The relationship began in 2010 with Towerwall serving as the college's consulting organization for endpoint protection and expanded recently into a strategic cybersecurity partnership.

Towerwall updated the college's Information Security Policy, performed a campus-network cybersecurity risk assessment, developed an incident response and recovery plan based on the NIST 2.0 framework, and conducted tabletop exercises.

HOW **TOWERWALL** HELPS

"My engagement with Towerwall started about 15 years ago," recalls the CIO. "Initially they started out as our antivirus vendor. At the time, I didn't realize the full suite of cybersecurity services they offered." This perspective changed when Pawlaczyk attended Towerwall's 2023 Information Security Summit.

"Towerwall CEO Michelle Drolet had invited me every year. When I finally attended, I quickly realized the breadth and depth of services they offered. At that point we engaged in conversations on how to grow the partnership. This year I joined the Summit as a panelist on IR and disaster recovery planning.

Recognizing the need for a tailored approach within budget constraints, Pawlaczyk worked closely with Towerwall. "I didn't have a huge budget... Michelle was very open to... 'Let's figure out what's the biggest return for the budget you have. If you're in crawl mode right now, how do we get you to walk and then to run mode.' Her approach resonated with what I was looking for."

"Security can be overwhelming. I wanted to move at a relatively quick pace and fast forward to the tabletop exercise. Greg Neville [Towerwall CISO] provided guidance, laying out a project timeline with appropriate goals and milestones, saying, you can't put the roof on the house until you've poured the concrete and built the frame. I just wanted to focus on the roof. Greg put the foundation in place."

KEY STEPS TO ENGAGEMENT WITH TOWERWALL:

“Our work with Towerwall followed a clear, step-by-step approach to strengthening our cybersecurity posture. It began with crafting a modern information security policy based on the NIST framework, which also ensured our GLBA compliance.“

“Next, they conducted a targeted assessment of our environment that aligned with the NIST standard. This assessment identified and ranked our cyber risks, leading us to prioritize incident response and user training as our immediate focus areas. We then developed a practical IR plan, complete with actionable playbooks for two key scenarios. To ensure readiness, the IT staff were trained on this new IR plan. The culmination was a realistic tabletop exercise designed and led by Towerwall. I assisted in the designing of the tabletop scenarios. Then during the actual exercise, I observed but didn't participate, allowing my team to practice stepping into unfamiliar roles and responding effectively without my direct guidance. Finally, we began developing a comprehensive cyber training strategy.”

This flexibility led to a focused engagement in delivering four key services:

1. Policy Development:

"They helped us rewrite our information security policy, which was somewhat dated." Towerwall provided essential updates and reporting on the program to formalize security governance, ensuring foundational policies aligned with current threats.

2. Cybersecurity Risk Assessment:

Towerwall conducted a targeted assessment to identify risks. Pawlaczyk initially wanted to skip this step, but Towerwall was firm, saying, “We can't work effectively with you until we've done a proper risk assessment. Even if it's just an abbreviated one, we need to understand where your risks are. Then we can advise you."

3. Incident Response Plan:

Implicit in the assessment and policy work was the refinement of Saint Michael’s incident response capabilities, forming a foundation for readiness. The assessment identified gaps informing the IR strategy, ensuring the college had actionable steps for potential breaches. The objective is to minimize downtime, protect assets, and ensure operational continuity.

4. Tabletop Exercises:

Simulating cyber incidents and identifying gaps. This practical exercise tested the updated policies and IR plan. Towerwall ensured foundational work preceded the exercise for maximum effectiveness. Improving response readiness is the goal.

OUTCOME AND PARTNERSHIP

Pawlaczyk was highly satisfied with the results. The engagement provided significant value within budget. **"Towerwall was very flexible with our budget constraints, and they delivered a good product."**

LOOKING FORWARD

The partnership with Towerwall has transformed Saint Michael's approach to cybersecurity. Looking ahead, Joe Pawlaczyk anticipates leveraging Towerwall's flexible, strategic guidance to navigate evolving threats. "Given the constant pressure from ransomware and the complexities of cloud security, we expect to explore how the firm can help us further strengthen our defenses and incident recovery capabilities."

The college also anticipates refining its policies and conducting regular tabletop exercises based on Towerwall's proven methodology to maintain readiness.

Reflecting on the journey from seeing Towerwall as just an antivirus vendor to recognizing them as a strategic security partner, Pawlaczyk concludes, **"Over a 15-year span, Towerwall would always reach out once or twice a year, just to check in. We're not a six-figure customer of theirs, but they make me feel like we are. When we have additional budget for cyber initiatives, they will be the first place I call. Towerwall is the real deal."**