BULLWALL

CUSTOMER STORY

PROVIDING RANSOMWARE RESILIENCE TO A HEALTHCARE ORGANIZATION

Industry
Healthcare

Location
Ireland

BullWall Champion
Bryan Smyth, ICT Manager

900
Staff

10,000
Families
cared For annually

10
Staff looking after the entire IT Infrastructure

OVERVIEW

In 2021, the Healthcare Service Executive (HSE) was hit by a major ransomware attack, which had some impact on The Coombe Hospital in Dublin. However, in December of the same year, The Coombe Hospital suffered its own ransomware attack, resulting in the encryption of their servers. Rather than negotiating with the attackers, the hospital opted to handle the recovery process internally. With a dedicated effort from all teams, it took three and a half months to fully restore all services. This recovery was gradual, with departments coming back online step by step, but full functionality across all areas was only achieved after this period.

EXPLOITING KNOWN WEAKNESSES

The team at The Coombe Hospital had already identified several areas in their systems that needed improvement, and a network infrastructure refresh was planned. However, this was delayed due to the earlier ransomware attack on the HSE, creating a window of opportunity for cybercriminals to strike. The attack on The Coombe occurred on December 16, just as the team were preparing for Christmas. With HSE staff still working seven-day weeks for the past six months to recover from their own cyberattack, they were only able to provide limited support.

> THE RANSOMWARE ATTACK ON THE COOMBE OCCURRED ON DECEMBER 16, **WHILE THE HSE STAFF WAS STILL WORKING SEVEN-DAY WEEKS RECOVERING FROM A PREVIOUS CYBERATTACK.**

REBUILDING AFTER THE ATTACK

Following the HSE ransomware attack, stringent security protocols were introduced to prevent future breaches. These included wiping and rebuilding every end-user device from scratch. Once the data was verified as clean, it was migrated to a separate, secure network. Additionally, all servers underwent thorough low-level analysis, requiring between 30-50 hours of manual scanning

overseen by the HSE's security partner. This rigorous process contributed significantly to the lengthy recovery time. Simultaneously, the hospital upgraded its network infrastructure, implementing a new IP system to ensure that only rebuilt devices could connect to the clean network, fully isolated from any potentially compromised systems. Post-attack investigations pointed to the VPN as the likely entry point for the breach. However, since the VPN files were destroyed during the attack, the hospital cannot confirm this with absolute certainty.

INTEREST IN BULLWALL GREW FURTHER UPON REALIZING THE HOSPITAL HAD STRONG AUDITING AND ALERTING SYSTEMS BUT **LACKED A WAY TO STOP MALICIOUS ACTORS WHO MANAGED TO BYPASS THE INITIAL PREVENTATIVE SOLUTIONS.**

SELECTING A SOLUTION TO GUARANTEE RESILIENCE

After the attack was resolved and normal operations resumed, the focus shifted to overhauling the network. Since the network's vulnerabilities had already been identified, documented, and communicated, a plan was in place, along with the necessary funding, to address them.

Adopting a "security-first" approach aligned with NIS and NIS2 standards, the implementation of new infrastructure has brought about significant improvements across the organization. For example, two-factor authentication (2FA) has been rolled out organization-wide for email access, and the added security layers have been met without resistance. To ensure a robust "last line of defense," Coombe consulted with trusted reseller partners and other Irish hospitals.

One solution that repeatedly stood out was BullWall. Interest in BullWall grew further upon realizing the hospital had strong auditing and alerting systems but lacked a way to stop malicious actors who managed to bypass the initial preventative solutions. BullWall has now been integrated into the hospital's security stack, addressing vulnerabilities at every layer. As Coombe put it, "It's in place as a security safety blanket, our last line of defense."

With their overhauled and improved network infrastructure, NIS certified support tool and 2FA in place, Coombe Hospital are more prepared than ever to face the actions of bad actors, and with BullWall Ransomware Containment installed, they know they've got built-in resilience to face any and all future ransomware threats.

> *Nobody's ever fully protected. That's why it's important to focus not just on protection, but on* ***response, recovery and how resilient you are to a cyber-attack,*** *rather than how protected you are.*
>
> ***Bryan Smyth***
> *ICT Manager, The Coombe Hospital*

ABOUT BULLWALL

BullWall is the pioneer in ransomware resilience, providing robust defenses against the relentless threat of ransomware. Our focus on the latest ransomware tactics uniquely addresses critical gaps left by other security solutions. By delivering server-based protection without an endpoint agent, BullWall keeps critical IT infrastructure secure and operational during the core stages of an attack – before, during and after.

Learn more at www.bullwall.com.

BULLWALL