<https://www.cassevern.com/casestudy/vulnerability-assessment-case-study-hospital/>

**Vulnerability Assessment Case Study for Hospital**

[< All Case Studies](https://www.cassevern.com/resources/case-studies)

**Challenge**

The client, a large regional healthcare center, needed to do an in-depth check on their security situation and assess their vulnerability to hackers and other threats. They turned to CAS Severn, their trusted advisor for IT, to handle the assessment and make recommendations of how to improve their security.

**Solution**

Vulnerability assessment and action plan

**Results**

* Issues of varying severity were discovered quickly, and the team notified hospital officials so they could take action immediately, rather than wait for the final report.
* Identified unknown entry points.
* Recommendations for standardization of infrastructure installations, configurations, and maintenance.
* Educated and increased staff awareness on what they could change to improve their security situation.
* Client had a Strategic action plan to keep their environment secure.

**Market:** Healthcare

**Solution Area:** Security

Our experts tested security infrastructure devices, network servers, operational systems (including Windows, AIX, and Linux), physical security of buildings, and wireless internet security. We also looked at policies, procedures, network entry points, and network infrastructure. The project spanned several months in order to provide the hospital with an accurate snapshot of their current security posture. Our team didn’t test things once and assume that what they saw was the norm, because anything can be anomaly for one day. We were looking for trends and recurring issues that needed attention.

We found issues of varying severity in many areas. As issues were uncovered our team notified hospital officials so they could take action immediately, rather than wait for the final report.

One main problem we uncovered was that the hospital needed a standard way of installing, configuring, and maintaining servers and infrastructure equipment. With a large organization, this is a common problem, as different departments and staff tend to have different ways of managing their IT. Putting in a set of procedures for the entire hospital helps eliminate threats.

We also discovered unknown entry points – both physical and electronic – that posed a threat to the overall confidentiality, integrity, and availability of network data and resources. We made recommendations on how to tighten security controls and eliminate unnecessary entry points that would greatly reduce the threat of outside intrusion.

Another benefit was a greater awareness among the entire IT staff about how any vulnerability or weakness in any functional area affects the overall security posture of the hospital at large.

Our team gave the hospital staff a full report on what we found and helped to educate their staff on what they could change to improve their security situation. With our help they had a strategic action plan for how to keep up with regular assessments to keep their environment secure.

**CAS Severn Value:** Our team has a wealth of experience working in the healthcare field. Our role as a trusted advisor means that we’re not trying to sell the client on a specific solution. We make expert, vendor-agnostic recommendations, based on our proven assessment methodology, that are in the best interest of the client’s IT security.