

## SARCOM Gives Small Community Hospital an IEM Assessment

**The Challenge:** Community Hospital requires an IEM Assessment.

This regional hospital is the flagship hospital in a Regional Health Systems. Started in 1959, the regional hospital became a private, not-for-profit healthcare facility in 1994. In the early days the hospital had only fifty employees and seven physicians on staff. The hospital experienced tremendous growth over the years and now has more than 1,000 employees and 150 physicians.

The hospital is proud to be one of the largest non-government employers in its county, and provides quality care in cancer treatment, cardiac care, same day surgery, orthopedics, diagnostics, women's health, rehabilitation services and much more.

They asked SARCOM to perform an IEM Assessment to review the INFOSEC posture of this small community hospital and identify potential vulnerabilities in its overall security program, operating procedures, security policies, and information systems. At the completion of the assessment, SARCOM provided recommendations for the elimination or mitigation of these vulnerabilities.

**The Solution:** The SARCOM plan achieves the hospital's objectives.

SARCOM's definition of a security policy is as follows: Policies, procedures, and practices designed to provide reasonable assurance that business objectives will be achieved and that undesired events will be prevented or detected and corrected.

SARCOM identified the following items as significant objectives for the security assessment engagement:

---

**The Challenge:** Community Hospital requires an IEM Assessment.

---

**The Solution:** The SARCOM plan achieves the hospital's objectives.

---

**The Results:** SARCOM's consistency rewards SARCOM and the hospital.

---

1. Determine which information is critical to the organization.
2. Identify the systems that process, store, or transmit that critical information.
3. Determine the proper INFOSEC posture for these systems
4. Identify potential vulnerabilities.
5. Recommend solutions to mitigate or eliminate those vulnerabilities.

The IEM Assessment was a technical process performed to determine the client's INFOSEC posture. This included the following items:

- Identifying exposed information through the identification and verification of customer information system assets.
- Identifying vulnerabilities to systems that process, store, or transmit critical information.
- Validate the actual INFOSEC posture for these systems.
- Recommend solutions to eliminate or mitigate identified vulnerabilities based on security objectives.

The engagement included the evaluation of the following areas:

- Port & SNMP Scanning - Port and SNMP scanning using Qualys. Documented responding devices and open ports/services.
- System Enumeration & Banner Grabbing- Documented device operating system using results from port scan.
- Wireless Enumeration - Discovered wireless network access points using Netstumbler or Kismet. Documented secured and open access points. Attempted to connect to unsecured access points to determine depth of possible wireless penetration.
- Vulnerability Scanning - Performed internal and external vulnerability scanning of all network devices using Qualys and ISS Internet Scanner vulnerability scanners. Produced vulnerability results reports from both scanners and write to CD.
- Firewall Analysis - Performed basic Firewall analysis by documenting mapping of external addresses to internal addresses and services that are available. Then SARCOM compared them to external vulnerability scan results to confirm external vulnerabilities.

**The Results:** SARCOM's consistency rewards SARCOM and the hospital.

At the completion of this project this community hospital, SARCOM provided a recommendations document for the elimination or mitigation of identified vulnerabilities in its security program, operating procedures, security policies, and information systems.