The Power of Protection: Medical Device Security

Cyber threats do not discriminate among industries, entities or individuals. As the healthcare industry increasingly finds itself at the heart of these attacks, medical device security can prove beneficial to combatting such dangers.

**POTENTIAL THREATS**

- **DIRECT ATTACK** (physical or wireless connection)
- **SOCIAL ENGINEERING** (insider knowledge of security or system measures)
- **MALWARE** (viruses, Trojans, worms)

**TARGETED THROUGH**

- **WEB SERVERS**
  - Data integrity compromised during transfer
  - Infected, integrated devices affecting greater network

- **DATABASE SERVERS**
  - External: Reverse engineering of publicly available device verification information
  - Internal: SQL injections

- **APPLICATION SOFTWARE**
  - Incompatibility or misconfiguration with legacy operating systems
  - Lack of timely updates

- **DIRECT ACCESS**
  - Weak or well-known passwords
  - Lack of physical device security
  - Active unused ports (USB)

**RISKS**

- **RECONFIGURATION OF DEVICE SETTINGS**
  - Equipment malfunction putting patient at risk

- **DATA THEFT AND MANIPULATION**
  - Loss of hospital and patient data
  - Altering of records

- **ACCESS TO INTERNAL NETWORKS**

**SOLUTIONS**

A secure system starts with a secure device. Be sure to:

- Close unused and unsecure ports
- Remove unneeded software
- Apply and maintain all third-party updates
- Configure to meet Center for Internet Security Benchmarks
- Design and develop using Secure Development Lifecycle (SDLC) best practices

**THE HEALTHCARE INDUSTRY**

- Has more than 50% of organizations with a Network Security score of a C or lower
- Ranks 15th out of 18th among all industries
- 75% of healthcare organizations were infected with malware from 8/2015–8/2016

According to an August 2016 SecurityScorecard report analyzing the security ratings of over 700 organizations in the healthcare industry.