Understanding the Terrorism Threats Posed to Medical Technology

Jason Brookbank

In the world today, terrorism represents a complex threat to the safe functioning of medical devices. The actions of terrorists could potentially lead to patient privacy violations, physical damage, device malfunctions, and equipment downtime. This all translates to lost revenue and the inability to properly diagnose and treat patients.

To help diminish the effects of a threat, one needs to understand the vectors, or routes, that an attack may take. There are two primary vectors that may be used: direct and remote access. Direct access is where an individual or group physically enters a site to perform their goal. Remote access is achieved via the Internet or access to the hospital's computer network via modem or wireless. Each attack vector may be blocked by a combination of passive and active security systems.

Gaining Direct Access

The direct access attack is probably the most disturbing of the vectors. This requires a person to physically enter a target facility. The intruder's goals can be anything from targeted theft of equipment, drugs, or even radioisotopes to tampering and sabotage of medical devices or facilities.

It is safe to assume that the intruder can duplicate the appearance of a legitimate entity. This can be the guise of a patient, facility staff, or even an external inspector. There have already been a sufficient number of occurrences where individuals claiming to be Joint Commission (JCAHO) surveyors attempted to gain access to hospital facilities.

To reduce the likelihood of an intrusion to any facility, there must be different layers of defense. The entrances and exits of the facility should be restricted in some manner so that it forces all unsecured individuals through the front door or other secured entrance.

The next layer is a physical token layer. This is typically a Photo ID tag that lists the name, department, and has a photograph of the subject. Some of the ID cards may contain a magnetic stripe, barcode, and/or radio frequency identification (RFID) tag. A system that logs doorway entries and exits can usually be bypassed through the use of an unnoticed, stolen card or a copied magnetic stripe or barcode.

The information layer takes the form of a password or pin number that the user commits to memory. These are often combined with the use of an ID card via a combined card reader and keypad.

The final layer is the personal interaction. This is where the official staff follows procedures for challenging individuals that they are not familiar with or that appear to be out of place. This layer acts as the final chance to catch someone before they do something that they should not.

Gaining Remote Access

The second means of attack is remote access. Most hospitals in developed countries are running internal computer networks. In turn, with the advent of large-scale digital image archive systems, the medical devices themselves are connected to the network. The attacks to a network can be either passive or active.

What Can You Do?

Here are some tips to promote safety at your facility:

- Ensure that all computer software is fully patched and updated in accordance with information technology and manufacturer policies. These include updates to operating systems, firmware, anti-virus software, and anti-spyware.
- Make sure computer backups occur regularly and are validated
- Change passwords and access codes on a schedule
- Perform random physical and network security audits
- Ensure that a employee termination security process is implemented. Close computer accounts, change locks, disable passkeys, and confiscate IDs.

Jason Brookbank is the president of Brookbank Biotech, Inc. in Grand Rapids, MI.

Passive attacks may come in the form of computer viruses, Trojans, worms, or spyware. Active attacks are from a group or individual that breaks into the network to gain control. At risk here are personal medical histories and worst of all, the incorrect functioning of medical equipment.[1] If medical devices are infected by a computer virus, it can cause the device to stop working or even malfunction, risking the patient and operator.

Having a layered security system, applied detailed security procedures, and uniform staff training concerning security will go a long way toward making your devices secure from terrorists.

Reference

1. **Messmer E.** Rx for patching mired in red tape. Network World. July 5, 2004. Available at: http://www.networkworld.com/news/2004/070504hospitalpatch.html. Accessed November 30, 2005.

Inside AAMI

Update to Medical Electrical Equipment Standard

ANSI/AAMI ES60601-1:2005, *Medical electrical equipment-Part 1: General requirements for basic safety and essential performance* is the third edition of the standard that covers any medical device that requires an electrical outlet or a battery. The AAMI/American National Standard edition is identical to IEC 60601-1:2005 with the exception that a few requirements have been modified to comply with the U.S. National Electrical Code (NEC) and relevant standards of the National Fire Protection Association.

To order the standard, visit http://marketplace.aami.org or call (800) 332-2264, ext. 217. The standard is available to AAMI members for $185 and non-members for $225. Order code: 606011-P; PDF order code: 606011-P-PDF. Source code: HI.

Executives Named to AAMI Staff Leadership Positions

Richard Gottwald, past president of the Plastics Pipe Institute, has joined AAMI as executive vice president, finance & administration and technical programs, while Leah Lough has been promoted from senior vice president, education and government programs to executive vice president, education and membership services.

"These moves enhance what is already an outstanding staff," says AAMI President Michael J. Miller, JD. "Rich brings fresh perspectives and a proven record of excellence, while Leah builds upon the superior work she has done for us over the past five years."

Company News

ZOLL Medical Enters Technology Agreement

ZOLL Medical has signed a three-year contract with Novation, a healthcare contracting services company that serves the purchasing needs of more than 2,500 members. The agreement covers the ZOLL AutoPulse(R) Non-invasive Cardiac Support Pump, and offers an opportunity for ZOLL's sales force to bring additional value to Novation's members, the company said. The agreement was reached after Novation's Nursing and Clinical Practice Council reviewed the AutoPulse using its new technology evaluation process. The Council found that the device was unique and proprietary in the market and offered incremental patient benefits. The AutoPulse is an automated, portable device comprised of a backboard and a simple, load-distributing LifeBand(R) that fastens across a victim's chest.

Study Focuses on Therapies

Medtronic has announced the first implants in the U.S. of the Medtronic ConcertoTM Cardiac Resynchronization Therapy Defibrillator (CRT-D) with Atrial Therapies. The clinical study is a prospective, non-randomized, multi-center, global clinical trial involving up to 425 patients at approximately 50 sites in Europe, the U.S., and Japan. The purpose of the study is to assess the safety and efficacy of atrial defibrillation therapy in patients with a current indication for CRT and implantable cardioverter defibrillator.