



IMPROVING PATIENT CARE WITH SECURE WIRELESS SYSTEMS FOR UNITED BRISTOL HEALTHCARE TRUST

United Bristol Healthcare Trust has been installing small, closely confined wireless systems since 2003 to provide specific services for clinicians on the wards and to overcome the challenges of providing temporary connectivity between different buildings. The Trust's objective, however, has always been to implement wireless solutions on a much greater scale throughout its nine hospitals - but only once a robust, scalable security infrastructure had been implemented. Working with their security integration specialist Peapod and their partner AirDefense, the Trust has found a safe way forward using wireless.

A challenging environment

Employing some 7,000 staff across nine different hospitals, United Bristol Healthcare NHS Trust (UBHT) is one of the largest acute trusts in the country as well as being a major teaching and research centre for the South West. In 2005, the Trust had over 110,000 inpatient and day case admissions. Dave Oatway is the Trust's Computer Services Manager, responsible for all operational IT services including support for 4,000 users and the introduction of new technologies and applications to meet clinical needs. His involvement with wireless dates back to 2003 when a number of small pilot systems were installed to overcome specific problems. In common with many other Trusts, UBHT is spread across several buildings and staff are quite frequently relocated from one building to another, often on a temporary basis.

The trust's location in the centre of Bristol adds to the challenge of providing connectivity; cabling between sites would mean tunnelling under busy roads, entailing disruption and high costs. Thus, one of the Trust's first wireless installations was a temporary system providing connectivity for a small group of people who had relocated to a different building. Another installation saw wireless being used within a ward to enable haematologists to use laptops – equipped with a barcode scanner – to scan patients' wristbands to check blood groups prior to treatment. With this type of application, data is available immediately on any laptop, avoiding any problems of lag time, for any member of staff or department that has a role in the care of that patient.



"We have to protect against threats. AirDefense enables us to do this."

Seeking a long-term solution for wireless security

As part of the Trust's implementation of the National Programme for IT, there is a commitment to utilise wireless throughout all the hospitals when clinical need justifies the use of the technology. Even with the small, early installations of wireless at Bristol, it had always been recognised that the IT department would need to tackle the issues of control and security associated with the technology before broader-ranging systems could be approved and rolled out across the hospital over a planned two year period. UBHT has been working with IT security specialists Peapod for a decade on a wide range of security integration projects. Early in 2005, Dave Oatway turned to Peapod for advice on identifying a robust approach to wireless which would offer guaranteed security and a foundation upon which more installations could be rolled out. Peapod advised them to consider utilising an AirDefense solution, who provided a demonstration of their proposed system and carried out a survey of the UBHT site, providing a report on what they had found.

Dave Oatway commented: "We were keen to work with an organisation that was independent of manufacturers, and AirDefense fitted this bill, as well as being recommended by Peapod. The ability of their solution to detect rogue access points was critical and more importantly deny them service was a feature which was missing from many other companies' offerings. A further important factor was that we felt AirDefense was the type of company with which we could develop a partnership and a long-term relationship – rather than just opt for a pure customer/supplier scenario".

The proposed system was designed to provide the Trust with a 'starter solution' which could be quickly and easily expanded as the number of wireless installations increased and budget became available. It is an overlay network to the Cisco infrastructure. In early 2006, an AirDefense wireless security appliance and two wireless sensors were installed; by mid 2007 there will be approximately 1,000 access points and 200 sensors. AirDefense Enterprise was installed to constantly monitor and ensure the security of the data over the network.

CASE STUDY | Healthcare



Wireless now and in the future

Since the AirDefense solution was implemented, Dave Oatway and his team have been able to detect when and where people are using wireless equipment and devices, as well as being able to automatically stop any unauthorised attempts to attach to the network. In addition, the system provides moment to moment details – presented as graphs – of traffic and potential threats, which will enable the Trust to identify and plan for future wireless installations. The Trust's growing number of wireless systems, which are viewed as being complementary to traditional cabling solutions, are predominantly being used in ward environments and in a theatre suite to provide a fast and efficient way of entering and retrieving patient data.

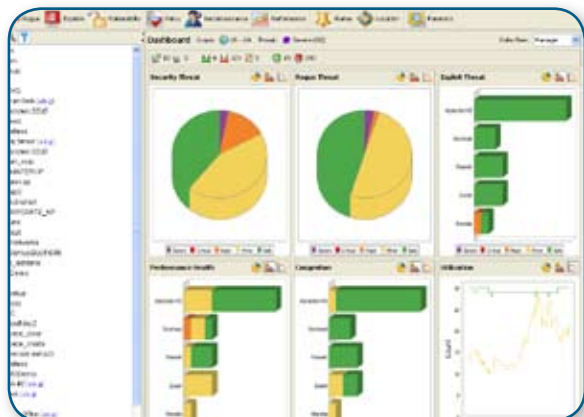
UBHT is also looking at introducing wireless telephones which will allow clinicians to speak to whoever is trying to contact them immediately – rather than having to respond to a pager at an available phoneline, all of which takes up valuable time. Another potential application is for the hospital's Intensive Care Unit. If someone is taken ill within the hospital and ideally needs to be moved to ICU – but there are no beds available – the requisite monitoring equipment can be taken down to the ward and then connected – using wireless – back to ICU. In this way, ICU staff will be able to monitor a patient with access to all their sophisticated equipment, without the patient having to be physically within the Unit. Given the pressure on beds in ICU, this has the potential to allow UBHT to offer improved care to a larger number of seriously ill patients.



A number of significant national projects are also being progressed, including PACS, a digital archiving and retrieval system for x-rays. With the plan to roll out this major new system on wireless, combined with the need to meet government timelines for this service, the need for a robust infrastructure and stringent security is of paramount importance. Dave Oatway is enthusiastic about the benefits and exciting applications that wireless can deliver within a hospital environment, but is keen to stress that patient data confidentiality can only be assured with the installation of a robust infrastructure, such as that recommended by Peapod and delivered by AirDefense. “With cabling there are obviously clearly defined boundaries and it is much easier to limit the risk of unauthorised access. At Bristol, we have thousands of people walking around our buildings every single day. Although the vast majority will be law-abiding, we have to protect against threats that we don't even know are out there. The AirDefense solution enables us to do this.”

About AirDefense, Inc.

AirDefense, the market leader in anywhere, anytime wireless security and monitoring, is trusted by more Fortune 500 companies, healthcare organizations and high-security government agencies for enterprise wireless protection. AirDefense products provide the most advanced solutions for rogue wireless detection, policy enforcement and intrusion prevention, both inside and outside an organization's physical locations and wired networks. Common Criteria-certified, AirDefense enterprise-class products scale to support single offices as well as organizations with hundreds of locations around the globe. Founded in 2001, AirDefense is based in Alpharetta, GA, and serves hundreds of government agencies and blue chip corporations.



AirDefense Dashboard

Row	Criticality	Category	Type	Detail	Start Time	Expiration
1	Severe (C2)	Rogue Endpoint	Rogue Station on Network	Unknown IP Address	11/25/08 11:09 PM	11/25/08 11:02 PM
2	Severe (C2)	Rogue Endpoint	Rogue Station on Network	216.104.142.11	11/25/08 9:31 PM	11/25/08 08:08 PM
3	Critical (C1)	KID: 11: Unauthorized	Device Unregistered to ...	Client Name: AP180	11/25/08 9:41 PM	11/25/08 04:41 AM
4	Critical (C1)	KID: 11: Unauthorized	AP & Non-AP Mode ...	Client Name: AP180	11/25/08 9:41 PM	11/25/08 04:41 AM
5	Critical (C1)	KID: 11: Unauthorized	Device Unregistered to ...	Client Name: S1	11/25/08 9:41 PM	11/25/08 04:22 AM
6	Critical (C1)	KID: 11: Unauthorized	AP & Non-AP Mode ...	Client Name: AP180	11/25/08 9:41 PM	11/25/08 04:22 AM
7	Critical (C1)	Authentication	AP Authentication Mode ...	Client Name: S1	11/25/08 10:54 PM	11/25/08 03:08 AM
8	Critical (C1)	Authentication	AP Authentication Mode ...	Client Name: S1	11/25/08 10:54 PM	11/25/08 03:08 AM
9	Critical (C1)	KID: 11: Unauthorized	AP & Non-AP Mode ...	Client Name: S1	11/25/08 10:54 PM	11/25/08 03:08 AM
10	Critical (C1)	KID: 11: Unauthorized	AP & Non-AP Mode ...	Client Name: S1	11/25/08 10:54 PM	11/25/08 03:08 AM
11	Critical (C1)	Authentication	AP Authentication Mode ...	Client Name: S1	11/25/08 10:54 PM	11/25/08 03:08 AM
12	Critical (C1)	Authentication	AP Authentication Mode ...	Client Name: S1	11/25/08 10:54 PM	11/25/08 03:08 AM
13	Major (C3)	Support Activity	Soft AP	AirDefense-002-0002	11/25/08 9:35 PM	11/25/08 03:01 PM
14	Major (C3)	Support Activity	Soft AP	Client Name: S1	11/25/08 9:35 PM	11/25/08 03:01 PM
15	Major (C3)	First Incident	Address Network Violation	Address: 11.11.11.11	11/25/08 9:35 AM	11/25/08 10:05 PM
16	Major (C3)	First Incident	NIDS: 11: Prohibited	Client Name: S1	11/25/08 10:05 PM	11/25/08 03:01 PM
17	Major (C3)	First Incident	Soft Prohibited IP	Client Name: S1	11/25/08 10:05 PM	11/25/08 03:01 PM
18	Major (C3)	Prohibited Problems	Unauthorized Station De ...	Client Name: S1	11/25/08 9:38 AM	11/25/08 03:01 PM
19	Major (C3)	Authentication Violation	Unauthorized Station in ...	Client Name: S1	11/25/08 9:38 AM	11/25/08 03:01 PM
20	Major (C3)	Support Activity	Handover PPK: 0000-00 ...	Client Name: S1	11/25/08 9:38 AM	11/25/08 03:01 PM
21	Major (C3)	Authentication Violation	Unauthorized Station in ...	Client Name: S1	11/25/08 9:38 AM	11/25/08 03:01 PM
22	Major (C3)	Authentication Violation	Unauthorized Station in ...	Client Name: S1	11/25/08 9:38 AM	11/25/08 03:01 PM
23	Major (C3)	Prohibited	Unauthorized Station in ...	Client Name: S1	11/25/08 9:38 AM	11/25/08 03:01 PM

AirDefense Alarm Manager